Article

On the Universal Encoding Optimality of Primes

Ioannis N. M. Papadakis

Independent Researcher, Charlotte, NC 28226, USA; ypap@primactaglobal.com

Abstract: The factorial-additive optimality of primes, i.e., that the sum of prime factors is always minimum, implies that prime numbers are a solution to an integer linear programming (ILP) encoding optimization problem. The summative optimality of primes follows from Goldbach’s conjecture, and is viewed as an upper efficiency limit for encoding any integer with the fewest possible additions. A consequence of the above is that primes optimally encode—multiplicatively and additively—all integers. Thus, the set $P$ of primes is the unique, irreducible subset of $\mathbb{Z}$—in cardinality and values—that optimally encodes all numbers in $\mathbb{Z}$, in a factorial and summative sense. Based on these dual irreducibility/optimality properties of $P$, we conclude that primes are characterized by a universal “quantum type” encoding optimality that also extends to non-integers.

Keywords: prime number; prime factor; factorization; optimization; integer programming; ILP; Goldbach conjecture; encoding; cryptography; quantum

1. Introduction

Prime numbers were a subject of mathematical inquiry long before the time of Pythagoras (570–500 BCE), who first attributed to numbers in general and their relationships a unique—almost mystical—power to express deeper truths about the universe and natural phenomena [1–3]. Although Pythagoras and his school did not systematically study primes, we refer to primes that can be expressed as sum of two squares, as “Pythagorean Primes”, e.g., $5^2 = 3^2 + 4^2$, $17^2 = 8^2 + 15^2$. The Greek philosopher Heraclitus (540–480 BCE) also accepted the existence of “powerful hidden harmonies” in nature and worked them into his philosophical theory about the cosmos [4]. The systematic study of primes starts with Euclid (fl. 300 BCE), who famously proved that primes “measure” all other numbers and that there is an infinitude of them [5,6]. Eratosthenes (276–194 BCE) invented a sieve as a practical way to find primes [7] by observing that composite numbers follow repeating patterns. Goldbach (1690–1764), Euler (1707–1783) and Riemann (1826–1866)—among other mathematicians—have grappled with important questions related to prime numbers. One of those questions, Goldbach’s conjecture, states that every even number $\geq 4$ can be expressed as a sum of two primes. It remains unproven despite “twenty-six decades of effort by some of the best minds on the planet” ([7], p. 90) as one of those “conjectural theorems of which no proof is known, although empirical evidence makes their truth seem highly likely” [8].

The increasing rise of digital communications in recent years, along with the concomitant need for enhanced privacy and secure authentication, has rekindled interest in prime numbers. Several encryption methods employ large primes in the construction of secure cryptographic keys, since the prime factorization of large numbers is a computationally tedious process. Primes therefore help secure the communication of digital information over public networks such as the internet [9].

Life patterns based on primes also occur in nature. Examples are the cicadas’ 13- and 17-year birth cycles, giving them an advantage over predators by making it rarer to coincide with them. If a predator emerges on a 5-year cycle, it will coincide with the cicadas every 65 and 85 years respectively, giving them an evolutionary advantage. Prime numbers can
help explain the phyllotaxis spirals, characteristic spiral arrangement of leaves that maximize a plant’s sunlight exposure.

Scientists continue to study the numerical, algebraic, geometric, distributional, asymptotic and other properties of prime numbers—proved or conjectured—and explore their implications on the nature of our universe.

In this paper, we show that the set $P \cup \{1\}$ has the smallest cardinality and values for optimally encoding all integers through product or sum operations. We refer to this unique dual irreducibility property or primes as a quantum type encoding optimality. Finally, we show how these encoding properties can be extended to non-integers.

2. ILP Formulation–Additive Optimality of Prime Factors

Euclid, in his Elements, first proved that any integer, larger than or equal to 2, that is not a prime can be expressed as a product of primes called prime factors ([5] Book VII Prop. 30–32, pp. 218–219; Book IX Prop. 14, p. 265). This result is of such profound importance in mathematics that it has been called the “Fundamental Theorem of Arithmetic”.

The uniqueness of prime factorization implies that an integer cannot be expressed factorially using a smaller number of prime factors. Primes can therefore be thought of as the “universal factorial quanta” of $Z_{\geq 2}$, and, in that sense, $P$ is irreducible in a quantum sense; i.e., no subset of $Z$ with smaller cardinality or member values exists having the same universally optimal factorial encoding capability in $Z$.

Irreducibility is a fundamental property in science; for mathematics in particular, irreducibility arises in problems related to computability, incompleteness, decidability, algorithmic information theory and the limits of computation [10]. Generally, when all members of a set $A$ can be expressed as functions of set $B$, and no set with smaller cardinality than $B$ exists with the same property, then $B$ is called irreducible. If $B \subset A$ and $B$ is irreducible in cardinality and values, i.e., if $B$ contains the fewest and smallest numbers possible, capable of encoding every member of $A$, we refer to the subset $B$ of $A$ as optimal in a quantum encoding sense.

Prime factors are also optimal in a factorial-additive sense, as we show below.

**Definition 1.** For $s \in Z_{\geq 2}$, the Prime Counting Function $\pi(s)$ is equal to the number of primes less than or equal to $s$.

**Notation.** The symbols $\mathbb{R}$, $Z$ and $Z_{\geq 2}$ are used in this paper as representations of the set of real numbers, integers and integers greater or equal to 2, respectively. The $n$th prime number, in ascending order, is denoted as $p_n$; $P_n$ is the set of the first $n$ primes, $P$ of all primes, $\hat{P} = P \cup \{1\}$, $P_o$ is the set of odd primes, and $\hat{P}_o = P_o \cup \{1\}$. The integer part of $x \in \mathbb{R}$, i.e., the largest integer less than or equal to $x$, is denoted by $\lfloor x \rfloor$ and the discrete delta function, taking the values of 1 for $x = 0$ and 0 for $x \neq 0$, is denoted by $\delta(x)$. The natural logarithm of $x$ is $\log(x)$.

**Example 1.** $\pi(12) = 5; \pi(13) = \pi(14) = \pi(15) = \pi(16) = 6$ where $P_5 = \{2,3,5,7,11\}$, $P_6 = P_5 \cup \{13\}$.

Consider an odd $s \in Z_{\geq 3}$ with $\pi(s) = n$ for some $n \in Z_{\geq 1}$; then $s$ may be expressed by its prime factorization

$$s = \prod_{i=1}^{n} p_i^{d_i}$$

where $p_i \in P_o, d_i \in Z_{\geq 0}$ for $i \in [1, n]$. By taking the natural logarithm on both sides of (1)

$$\log(s) = \sum_{i=1}^{n} [d_i \cdot \log(p_i)]$$
and since \( s \geq p_n > n \), the above may be written as

\[
\log(s) = \sum_{\substack{i = 3 \\ i \equiv \text{odd}}}^{s} \tilde{d}_i \log(i)
\]

or, equivalently, in vector form

\[
\log(s) = \tilde{d}_s^T \log(s)
\]

where

\[
\tilde{d}_i = \begin{cases} 
    d_i & \text{if } i = p_i \\
    0 & \text{if } i \neq p_i
\end{cases}
\]

\[
\bar{s} = \begin{bmatrix} 
    3 \\
    5 \\
    \vdots \\
    s - 2 \\
    s
\end{bmatrix}
\]

By applying (2) on each element of \( \log(s) \) we obtain

\[
\log(s) = \begin{bmatrix} 
    \tilde{d}_1^T \\
    \vdots \\
    \tilde{d}_n^T
\end{bmatrix} \log(s) = \tilde{D}_s \log(s)
\]

where

\[
\log(s) = \begin{bmatrix} 
    \log(3) \\
    \log(5) \\
    \vdots \\
    \log(s - 2) \\
    \log(s)
\end{bmatrix}
\]

and \( \tilde{D}_s \in \mathbb{Z}_{(s-1)/2 \times (s-1)/2}^{>0} \) is the augmented log coefficient matrix of \( s \). The following example shows how (3) can be used to compactly express the prime factorizations of all odd numbers in \([3, s]\).

**Example 2.** Consider \( s = 9 \). Using (3), the logarithm of each odd \( i \in [3, 9] \) can be expressed through prime factorization as a linear product of \( \log(s) \), as follows:

\[
\begin{bmatrix} 
    \log(3) \\
    \log(5) \\
    \log(7) \\
    \log(9)
\end{bmatrix} = \begin{bmatrix} 
    1 & 0 & 0 & 0 \\
    0 & 1 & 0 & 0 \\
    0 & 0 & 1 & 0 \\
    2 & 0 & 0 & 0
\end{bmatrix} \begin{bmatrix} 
    \log(3) \\
    \log(5) \\
    \log(7) \\
    \log(9)
\end{bmatrix}
\]

In the above equation, \( \log(9) \) is expressed through the prime factorization of \( 9 = 3^2 \), or equivalently

\[
\log(9) = 2 \cdot \log(3)
\]

and not via the identity

\[
\log(9) = 1 \cdot \log(9)
\]

which would result in \( \tilde{D}_s = I \). This is an important distinction, in terms of the additive optimality of prime factors, as we will see below.

We can rewrite (3) as

\[
[\tilde{D}_s - I] \log(s) = \nabla
\]
where I is the \((s - 1)/2 \times (s - 1)/2\) identity matrix and \(\vec{0}\) the \((s - 1)/2 \times 1\) null vector. Equation (4) implies that the vector \(\log(\vec{s})\) is in the null space of matrix \(D_s^{-1}\). As we saw in the previous example, this does not give us immediate insight into the optimality of \(D_s\), since \(D_s = \vec{1}\) trivially satisfies (4). To establish the additive optimality of prime factors we need the following proposition.

**Proposition 1.** Let \(D_s\), \(\vec{s}\) satisfy (4). If \(\tilde{D}_s\) corresponds to the prime factorization of \(\vec{s}\), then every element of the \((s - 1)/2 \times 1\) vector \(\tilde{D}_s \cdot \vec{s}\) attains its minimum value.

**Proof.** Since the minimality applies element-wise for vector \(\tilde{D}_s \cdot \vec{s}\), we may use (2) to show that the proposition holds for each vector element. Consider any non-prime factorization of a composite, i.e., non-prime, number \(s > 1\) and let \(q\) be any composite factor. If \(s\) is odd, 2 cannot be one of its factors, and it follows that there is a prime \(p > 2\) and some odd integer \(q > 2\) such that \(s = p \cdot q\). Using basic algebra, we can show that \((p + q) < p \cdot q = s\), i.e., the sum, \(p + q\), of two factors is always strictly less than their product \(p \cdot q\) iff \(1/p + 1/q < 1\) which, in this case, is true. Since primes are the smallest factors possible, the proposition is proved. For \(s\) even, the same rationale applies with the exception that, in this case, we have \(p \geq 2\) and \(q \geq 2\) so that \((p + q) \leq p \cdot q = s\). Therefore, in this case, the attained additive minimum may not be unique, except for the special case when \(s/2\) is odd. □

**Remark 1.** The minimality condition of Proposition 1 does not extend to the logarithms of composite factors, since

\[
\log(p) + \log(q) = \log(p \cdot q) = \log(s).
\]

**Remark 2.** The reason for losing the strict inequality in the proof of the above proposition for \(s\) even—and thus, the uniqueness of the minimum—is that the number 2 has the unique property \(2 \cdot 2 = 2 + 2\), which means that any factorization having \(2^n\) as a factor, with \(n \geq 2\), results in different factorizations with equal factor sums. For example, consider \(s = 2^3\), which can be factored either as \(2 \cdot 4\) or \(2 \cdot 2\cdot 2\), both with a factor sum of 6. Even numbers not divisible by \(2^n\), for \(n \geq 2\), are not subject to this relaxation. In such case, \(s/2\) is odd, since the multiplicity of 2 in the prime factorization of \(s\) is equal to one. As a result, the conditions for the strict inequality in the proof of Proposition 1 hold.

**Example 3.** Consider \(s = 450\) with prime factorization \(2^1 \cdot 3^2 \cdot 5^2\) and prime factor sum equal to \(1 + 2 + 3 + 2 + 5 = 18\). From the previous discussion, we expect non-prime factorizations to have factor sums larger than that of prime factors:

\[
\begin{align*}
2 \cdots 225 & \rightarrow 2 + 225 = 227 > 18 \\
18 \cdots 25 & \rightarrow 18 + 25 = 43 > 18 \\
2 \cdots 9 \cdots 25 & \rightarrow 2 + 9 + 25 = 36 > 18 \\
6 \cdots 3 \cdots 5 \cdots 5 & \rightarrow 6 + 3 + 5 + 5 = 19 > 18 \\
2 \cdots 3 \cdots 3 \cdots 5 \cdots 5 & \rightarrow 1 \cdots 2 + 2 \cdots 3 + 2 \cdots 5 = 18
\end{align*}
\]

This example demonstrates how the sum of factors gradually decreases as each factorization includes more prime terms, attaining its unique minimum value (=18) when all factors are prime numbers.

The additive minimality of prime factors, established by Proposition 1, gives us additional insight into how efficiently primes encode integers in a factorial-additive sense.

**Example 4.** Consider the previous example and suppose we are asked to encode \(s = 450\), using multiplication only, in a way that minimizes the “additive cost” of the factors used to generate it.
We are told that each factor has a cost equal to its value and are asked to allocate our factor-cost budget in such a way that 450 is generated factorially at minimum cost. The unique solution to this encoding optimization problem is to generate 450 via its prime factorization $450 = 2^1 \cdot 3^2 \cdot 5^2$ at a total additive-cost of 18. The additive cost of every alternate factorization is higher than that of the prime factors, ranging from 19 to 227, as shown in the previous example.

In summary, the subset $\hat{P} \subset \mathbb{Z}$ uniquely encodes all members of $\mathbb{Z}$ factorially, has the lowest cardinality, the smallest possible numbers as members, with each factorial encoding also optimal in an additive sense.

From (4) and Proposition 1, it follows that prime factorization is the solution to the ILP-type problem

$$\min_{\tilde{D}_s} \left( \tilde{D}_s \cdot \vec{s} \right) \text{ elementwise subject to : } \left[ \tilde{D}_s - 1 \right] \log(\vec{s}) = \vec{0}$$

(5)

where $\tilde{D}_s \in \mathbb{Z}^{(s-1)/2 \times (s-1)/2}$.

Equation (5) describes a minimization problem with a linear objective function, linear constraints, and integer decision variables. Here, the decision variables are the elements of the augmented log coefficient matrix $\tilde{D}_s$.

Remark 3. The last row of $\tilde{D}_s$ corresponds to the prime factorization of $s$, expressed in log form, as in (2).

Observe that the value of element $\tilde{D}_s[i,j]$ of matrix $\tilde{D}_s$ can be constrained by

$$\tilde{D}_s[i,j] \leq \frac{\log(2i + 1)}{\log(2j + 1)} \text{ if } i \geq j \text{ and } \tilde{D}_s[i,j] = 0 \text{ if } i < j$$

(6)

to further reduce the size of the ILP’s decision space.

Through the ILP formulation described by (5) and (6), we can employ a rich array of computational optimization methods to solve large-scale prime factorization problems.

Remark 4. The above formulation can be used to determine prime factors larger than a given number $n$. One way to accomplish this is to construct a number $s$ that cannot have any prime factor $\leq n$ and then solve the corresponding prime factorization ILP. A candidate that meets this condition is

$$s = M_n = \hat{n}! - 2^m$$

(7)

where $\hat{n}!$ is the product of all odd integers up to $n$ and

$$m = \left\lfloor \frac{\log(\hat{n}!)}{\log(2)} \right\rfloor$$

If $M_n$, given by (7), had any prime factors $\leq n$, it would follow that $2^m$ would have at least one of those as prime factor; false, since the only prime factor of $2^m$ is 2.

Example 4. To illustrate this point, consider the cases $m = 5, m = 13$:

$$M_5 = 5! - 2^5 = 120 - 32 = 88 \quad (\text{prime } > 5)$$

$$M_{13} = 13! - 2^{17} = 6227020800 - 2^{17} = 4063 = 17 \cdot 239 \quad (\text{bothprime } > 13).$$

For much larger $n$, finding the prime factors requires more sophisticated search and optimization techniques.
Remark 5. Instead of multiplying all odd numbers up to \( n \), as in the previous example, we can multiply the number 3 with all integers not exceeding \( n \), of the form \( 6k \pm 1 \) with \( k \geq 1 \), since all primes > 3 may be expressed that way. This results in a smaller candidate compared to \( M_n \). If we know the first \( m \) primes and want to search for a prime larger than \( p_m \), we can opt for an even smaller product given by \( \prod p_i \), where \( i = 2, 3, \ldots, m \). We explore additional search techniques in the next section, where we discuss partitions and the summative optimality of primes.

Remark 6. Given that any number \( s \in \mathbb{Z} \geq 2 \) may be written as

\[
s = \prod_{i=1}^{n} p_i^{d_i}
\]

where \( d_i \in \mathbb{Z}^{\geq 0} \) for \( i \in [1, n] \) are the factor exponents and since, by definition, all \( p_i \geq 2 \)

\[
s \geq \sum_{i=1}^{n} (d_i \cdot p_i)
\]

which implies that \( s \) is an (elementwise) upper bound on the factor-cost vector \( \tilde{D}_s \)’s given by (5).

Remark 7. The prime counting function \( \pi(\cdot) \) may be expressed in algebraic form. By using such an expression, we can express Goldbach’s Conjecture (GC) algebraically. In Appendix A, we derive algebraic expressions for \( \pi(\cdot) \) and GC and discuss their properties.

3. Summative Optimality of Primes

Of the many remarkable properties prime numbers possess, perhaps the most intriguing is a “mirroring” property inherent in their distribution on the number line. To visualize this, consider an even number \( s \geq 6 \), and write the odd numbers in \([3, s/2]\), in ascending order, on the left and those in \([s/2, s-3]\) in reverse order on the right. By construction, the sum of both elements in any row is equal to \( s \). In this otherwise unremarkable arrangement, at least one of the pairs is comprised of two prime numbers, suggesting that any even number \( s \geq 6 \) may be expressed as a sum of two odd primes.

Considering that the density of primes \( \pi(s)/s \) decreases as \( s \) is increased, the above conjectured “mirroring” property becomes even more surprising: that for any even number \( s \), there is always an odd prime in \([s/2, s]\) that “aligns” itself with another odd prime in \([3, s/2]\), in such a way as to partition \( s \). We will explore the implications of this later in the paper.

Example 5. Let \( s = 40 \) and consider all partition pairs \((q_L, q_R)\) where \( q_L \leq q_R \) with \( q_L, q_R \) odd > 1: \((3,37)^*, (5,35), (7,33), (9,31), (11,29)^*, (13,27), (15,25), (17,23)^*, (19,21)\). There are 3 \( P_o \times P_o \) pairs, marked with *.

Remarkably, after removing all repeating number patterns, such as the prime factors of \( s \) and their multiples, there is always an odd prime in \([s/2, s-3]\) that aligns itself with another odd prime in \([3, s/2]\) to form a partition of \( s \). This persistent pattern seems to be a fitting example of an Heraclitean “hidden universal harmony”.

An interesting ramification of the above, is that given an even \( s > 6 \) with \( m \) prime factors, at least one of the \( \pi(s/2) - m \) numbers given by \( s - p_i \), where \( p_i \) is any of the primes in \([3, s/2]\) that are not factors of \( s \), is prime. This facilitates finding large primes, as it dramatically reduces looking for prime candidates in \([s/2, s-3]\). Since a prime in \([s/2, s-3]\) is always paired with a prime number in \([3, s/2]\) which is not a prime factor of \( s \), if we want to find a prime larger than \( s/2 \), we need only perform at most \( \pi(s/2) - m \) primality tests. When we have no a priori knowledge of the primes in \([1, s/2]\) we may still use the algebraic properties of pairs in a partition to make the search for \( P_o \times P_o \) pairs more efficient. We discuss this in Appendix B. Note that a consequence of the prime density
decreasing with $s$ is that—even for large values of $s$—primes are not evenly distributed in $[1, s/2]$ and $[s/2, s]$; this is discussed in Appendix C.

This prime “mirroring” (or “pairing”) property is a result of the “Goldbach conjecture” (GC), named after the German mathematician Christian Goldbach (1690–1764) who mentioned it in a 1742 letter to the eminent Swiss mathematician, physicist, astronomer, geographer, logician and engineer Leonhard Euler, to which Euler responded: “That every even integer is a sum of two primes, I regard as a completely certain theorem, although I cannot prove it.” [11]. While Goldbach considered $1$ as prime, the statement “every even number $> 2$ can be expressed as the sum of two primes” is now the proper formulation of the GC, commensurate with our current definition of primes.

The GC is easily seen to imply that “every odd number $> 5$ is the sum of three primes”, since every odd number $> 5$ can be expressed as sum of an odd prime and some even number, which in turn is a sum of two primes. This is often referred to as the “weak” or “odd” Goldbach Conjecture (oGC).

In the two and a half centuries since the GC was formulated, and while considerable efforts have been made by mathematicians towards a proof, the conjecture remains open. The oGC is considered “relatively easier” and has been proved for numbers larger than $10^{43000}$ [12]. The GC has been computationally verified for numbers up to $4 \cdot 10^{18}$ [13].

Rather than considering the GC or oGC as binary questions, it is helpful to think of them, respectively, as encoding efficiency limits, in the sense that, in general, an even number cannot be written as a sum of fewer than two odd primes and an odd number cannot be written as a sum of fewer than three primes. In that sense, significant progress has been made towards attaining these encoding limits. Vinogradov (1937) showed that every sufficiently large odd integer can be written as the sum of at most three primes, and so every sufficiently large even integer is the sum of a prime plus a number with no more than two prime factors. The GC has also been linked to the Riemann Hypothesis (RH), in the sense that if we accept the RH as true, then every odd integer is a sum of three primes, which implies that every even integer is a sum of four primes. The interested reader can find more information in [14].

Ultimately, this might be the first instance where an important proof relies on showing a mathematical proposition to be true for a range of numbers larger than some lower bound $L$, while computationally confirming its validity for all numbers up to $L$.

In this paper, our purpose is to explore the universal optimality property of primes at its limit; we do so by assuming that the optimal encoding efficiency implied by the GC is true.

Note that, even at suboptimal encoding efficiencies, i.e., assuming that even (odd) integers can be expressed as sums of more than two (three) primes, the set of primes $P$ remains the subset of $Z$ with the fewest and smallest members that can most efficiently encode all integers. For example, consider the—suboptimal to the GC—summative encoding efficiency resulting from Bertrand’s postulate ([8], p. 455), which asserts that there is always a prime $p \in [n, 2n]$ where $n \geq 1$. Therefore, there is always a prime $p \geq s/2$ in the interval $[2, s]$ for $s \geq 3$. The postulate implies that this prime spans at least half of $s$. By successively applying this process we establish the existence of a sequence of decreasing primes $p_i$ with $s$ as its sum. For example, let $s = 100$ and let $p_1 = 61$ be the first prime in the sequence between $s/2, s$. By applying the postulate to the remainder $r_1 = 100 − 61 = 39$ and selecting $p_2 = 23 \in \{39/2, 39\}$ as the second term in the sequence, the new remainder becomes $r_2 = 100 − 61 − 23 = 16$. Since the new remainder is small (<20), we can easily express it as a sum of two primes, e.g., $13 + 3$. Generalizing, we can show that any number $s \geq 3$ can be written as a sum of at most $\lfloor \log(s)/\log(2) \rfloor + 1$ primes. Given the sparsity of primes and, hence, the low value of the ratio $n/p_n$, as $n$ increases, i.e., the ratio of the cardinality $n$ of $P_n$ to its largest member $p_n$, this demonstrates the remarkable summative encoding capability of primes.
We therefore accept as true that every even integer > 4 is a sum of two odd primes. Equivalently, we accept as true that every integer > 0 may be expressed as a sum of up to three numbers in $\mathbb{P}_n$. From the above discussion, it follows that by accepting the validity of the GC, we establish the significance of $\mathbb{P}_n$ and its subsets as the most efficient—in an encoding sense—“building block” of all integers, including primes themselves.

Note that, since $P \subset \mathbb{Z}$, we may apply the oGC to generate a “summative decomposition” of primes. Since each prime $\geq 5$ can be written as a sum of three primes, it follows that ultimately, smaller primes could be used as the summative building blocks of larger primes. For example: $5 = 2 + 3$, $7 = 2 + 2 + 3$, $11 = 3 + 3 + 5$, $13 = 3 + 5 + 5$, $17 = 5 + 5 + 7$, $19 = 5 + 7 + 7$, $23 = 5 + 7 + 11$ etc. We can therefore use the first 5 primes $\{2, 3, 5, 7, 11\}$ to summatively optimally encode the next 4 primes $\{13, 17, 19, 23\}$, for an intra-prime summative encoding efficiency factor of 1.8 [=9/5].

As with the factorial case, the optimal summative encoding implied by the GC can be represented as the solution of an optimization problem. In this case however, the formulation is nonlinear, i.e., gives rise to a nonlinear programming (NLP) formulation. To see this, consider how a set of even numbers in $[6, 2^m)$, generated by using one addition operation over the smallest possible subset of odds within $[3, 2^m - 3]$. The solution is the summative optimal encoding implied by the GC, i.e., that every even number $\geq 6$, is the sum of two primes.

Note that additional constraints may be introduced to refine this solution, when multiple summative encodings of an even number $e$ exist. One approach is to select the one with the smallest (or largest) deviation from the midpoint $e/2$, as discussed in Appendix B. For example, in the case of $e = 16$, this would result in $13 + 3 = (8 + 5) + (8 - 5)$ be more (or less) preferable than $11 + 5 = (8 + 3) + (8 - 3)$, in the sense that in the first encoding instance the distance from the midpoint is 5, while in the second it is equal to 3.

Let $\mathbf{w}_e$ be the vector of even numbers in $[6, 2^m)$, for some integer $m \geq 3$, and $\mathbf{w}_e$ the vector of odds in $[3, 2^m - 3]$. Thus, the NLP may be formulated as follows:

\[
\max_A \left[ \sum_{i,j} \delta \left( \sum_i a_{ij} \right) \right] \text{ subject to: } A \cdot \mathbf{w}_e = \mathbf{w}_e \text{ and } \sum_j a_{ij} = 2 \ \forall \ i
\]  

where $A$ is the $m \times m$ decision-variable matrix, with elements $a_{ij} \in \{0, 1, 2\}$ for $i, j \in [1, m]$, specifying the elements of $\mathbf{w}_e$ to be added in order to optimally generate the output vector $\mathbf{w}_e$. From the GC, we know that the prime elements of $\mathbf{w}_e$ are necessary and sufficient for an optimal NLP solution to exist, i.e., to satisfy the objective function and the constraints in (9).

Ongoing research is focused on alternate formulations, e.g., based on an objective function that minimizes the rank of the decision matrix, as in the NLP below:

\[
\min \text{rank}(A) \text{ subject to } A \cdot \mathbf{w}_e = \mathbf{w}_e, \sum_j a_{ij} = 2 \text{ for } i, j \in [1, m]
\]

4. Quantum Encoding Optimality

As we showed in Section 2, prime factorizations are optimal in a factorial-additive sense, since for any integer, the sum of its prime factors is minimum. Prime factors are irreducible in value, since there can be no factors smaller than prime factors. Thus, $P$ is an irreducible (in cardinality) subset of $\mathbb{Z}$ that can factorially encode all integers $> 1$ using factors that are also irreducible (in value) and have a minimal sum (factorial-additive optimality). From Section 3, it follows that the set $\mathbb{P}_n$ has an additional optimality property: it is the “smallest” (in cardinality) subset of $\mathbb{Z}$ whose members can summatively optimally encode any integer in $\mathbb{Z}$, i.e., with no more than two addition operations.

Combined, the factorial-additive and summative optimality of $\mathbb{P}_n$ empower its members with a unique “quantum-type encoding optimality”. The corollary below summarizes this result.

**Corollary 1.** $\mathbb{P}_n$ is optimal in a quantum encoding sense for all numbers in $\mathbb{Z}$. 


Proof. In Section 2, we showed that prime factorization is the optimal quantum factorial-additive encoding for any integer; that is, a factorial encoding that is also factorial-additively optimal uses the smallest possible factors that are members of an irreducible subset \( \hat{P} \) of \( \mathbb{Z} \), i.e., with the smallest possible cardinality. In Section 3, we discussed the summative-optimality of primes, and we explained how the GC expresses a summative encoding efficiency limit, with any integer encoded as a sum of up to three members of \( \hat{P} \). Thus, \( \hat{P} \) is the unique, irreducible subset (minimal cardinality) of \( \mathbb{Z} \), having members with irreducible (minimal) values, capable of optimally encoding any number in \( \mathbb{Z} \) in a factorial-additive and summative sense. □

Observe that there may be different ways to encode an even number using one addition in \( \hat{P}_o \), e.g., \( 11 + 5 = 13 + 3, 19 + 1 = 17 + 3 = 13 + 7, 19 + 3 = 17 + 5 = 11 + 11 \). Could this summative encoding redundancy point to an inherent robustness in nature?

Note that, for a number \( s \) with multiple summative prime decompositions, these may be ordered according to the product value of the summands, e.g., for \( s = 14 \) we have \( 7 \times 7 = 49, 3 \times 11 = 33 \). We call each product the prime summand product (PSP). Every \( s \) has a summative decomposition where the PSP obtains its minimum/maximum values. This is analogous to the factorial-additive minimum discussed in Section 2. See Appendix B for a discussion about the extrema of PSP.

In natural systems, redundancy is usually an evolutionary “insurance policy” to ensure survival, that is, continued performance under high uncertainty or risk. Fault-tolerance in AI systems is also a direct result of robust design. How much do the summative encoding capabilities of \( \hat{P} \) degrade if some of its members are eliminated? The answer may provide us with insights that lead to improvements in the design of robust, fault-tolerant systems.

5. Conclusions

The factorial-additive and summative optimality properties of primes, combined with their dual irreducibility (“quantumness”) in cardinality and value, provide us with unique insights into their ability to efficiently encode the seemingly innumerable patterns of quantifiable variability within our universe. This universal, powerful capability is amplified even more if we consider how low the density of primes \( \pi(x)/x \) is. For \( x \approx 10^3 \), prime density is approximately 17%; for \( x \approx 10^{13} \) it decreases to 3%, and for \( x \approx 10^{27} \) drops to 1.26%. Therefore, 98.74% of integers in \([1, 10^{27}]\) can be generated optimally—in a factorial and summative sense—by using only 1.26% of them! Prime numbers seem to be nature’s optimal encoding quanta of choice.

The set \( \hat{P}_o \) may also be used to encode irrational and transcendental numbers in a summative sense. For example, let’s consider \( \pi = 3.14159 \ldots \) By using the Leibniz formula for \( \pi \), written as an Euler product, \( \pi \) may be expressed as a product of ratios of odd primes divided by their nearest multiple of 4, as follows

\[
\pi = \frac{3}{4} \cdot \frac{5}{4} \cdot \frac{7}{8} \cdot \frac{11}{12} \cdot \frac{13}{16} \cdot \frac{17}{20} \cdot \frac{19}{24} \cdot \frac{23}{28} \cdot \ldots
\]

or equivalently

\[
\pi = \frac{3}{1+3} \cdot \frac{5}{1+3} \cdot \frac{7}{3+5} \cdot \frac{11}{5+7} \cdot \frac{13}{5+7} \cdot \frac{17}{3+13} \cdot \frac{19}{3+13} \cdot \frac{23}{5+19} \cdot \frac{29}{5+23} \cdot \ldots
\]

Since \( \hat{P}_o \) can summatively optimally encode every integer, it follows that it can also encode any product, ratio, sum or difference between integers.

Additional research work is needed to more fully explore the scope of the universal quantum-encoding optimality of prime numbers which enables this sparse subset of \( \mathbb{Z} \) to quantum-optimally encode any measurable quantity in the universe, to any desired degree of accuracy.

Funding: This research received no external funding.
Institutional Review Board Statement: Not applicable.
Informed Consent Statement: Not applicable.
Data Availability Statement: Not applicable.

Acknowledgments: The author expresses his gratitude to his doctoral advisor, Stelios C. A. Thomopoulos, Head of the Integrated Systems Laboratory and past Director of the Institute of Informatics & Telecommunications at the National Center for Scientific Research “Demokritos”, Greece, for his continued and invaluable mentorship. The author thanks Igal Sason, Professor at the Technion—Israel Institute of Technology, for his helpful comments at an early stage of this work.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. Two Closed-Form Expressions for the Prime Counting Function and an Algebraic Formulation of the Goldbach Conjecture

There exist several formulas for the prime counting function $\pi(\cdot)$, some containing a finite or infinite number of terms ([8], p. 593), [11,15]. Closed-form formulas, i.e., expressions with a finite number of terms, typically employ the modulo function $\mod(\cdot)$ and/or the factorial function ($\cdot)!$. Below, we derive two expressions for $\pi(\cdot)$ that use the integer-part operation, which may be approximated by smooth functions.

Proposition A1. Consider any integer $s \in \mathbb{Z} > 3$. Then $s$ is prime if and only if $T_s = 0$, where

$$T_s = \sum_{i=2}^{\lfloor s/2 \rfloor} \left\lfloor \frac{s/i}{s/i} \right\rfloor \quad (A1)$$

Proof. The ratio term $|s/i|/(s/i)$ in (A1) takes the value 1 only if $i$ is a factor of $s$, and some value in the interval (0,1) if $i$ is not a factor of $s$. Therefore, the integer part of this ratio is equal to 1 if $i$ is a factor of $s$ and 0 if it is not. Summation over all possible factors $i$ of $s$ up to $[s/2]$ implies that $T_s$ is nonzero if and only if $s$ is divisible by some integer in the interval $[2, s/2]$, i.e., $s$ is not prime. Therefore, $T_s = 0$ can only occur if $s$ is prime. □

$T_s$ has the properties of a “prime blocking filter”, e.g.,

$$y = T_s \cdot s$$

with pass-through properties for composite inputs ($T_s \neq 0$, composite $s$) while prime valued inputs are blocked ($T_s = 0$, prime $s$).

$T_s$ also expresses a primality test for $s$ in closed-form, so we can apply it iteratively and obtain a closed-form expression for $\pi(s)$.

Proposition A2. Consider any integer $s \in \mathbb{Z} > 3$. The prime counting function $\pi(s)$ is given by

$$\pi(s) = \sum_{j=2}^{s} \left\lfloor \frac{1}{1 + T_j} \right\rfloor = \sum_{j=2}^{s} \left\lfloor \frac{1}{1 + \sum_{i=2}^{\lfloor j/2 \rfloor} \frac{1}{i}} \right\rfloor \quad (A2)$$

Proof. Equation (A2) is an iterative application of the primality test given by (A1) for each $j \in [2, s]$ and factors $i \in [2, \lfloor j/2 \rfloor]$. From Proposition A1, the summand term $|1/(1 + T_j)|$ takes the value 1 if $j$ is prime ($T_j = 0$), or the value of 0 if $j$ is not prime ($T_j = 1$), and the proposition is proved. □

Another closed-form formulation for $\pi(s)$ follows from the proposition below.
**Proposition A3.** For any \( s \in \mathbb{Z} > 3 \)

\[
\pi(s) = \sum_{j=2}^{s} \left[ 1 - \delta \left( \prod_{i=2}^{\lfloor s/2 \rfloor} ((j/i) - \lfloor j/i \rfloor) \right) \right]
\]  

(A3)

**Proof.** Since the term \((j/i) - \lfloor j/i \rfloor\) is 0 if and only if \( i \) is a factor of \( j \), the product term in (A3) is zero if and only if \( j \) is not prime. In that case, \( \delta(0) = 1 \) and the value of the summand term is 0. Conversely, if \( j \) is prime, the product term is nonzero and the summand term is 1, thus counting \( j \) in the running sum. \( \square \)

The primality test associated with (A3) is

\[
\hat{T}_s = 1 - \delta \left( \prod_{i=2}^{\lfloor s/2 \rfloor} ((s/i) - \lfloor s/i \rfloor) \right)
\]  

(A4)

where \( \hat{T}_s = 0 \) if \( s \) is divisible by some \( i \in [2, \lfloor s/2 \rfloor] \), i.e., \( s \) is a composite number, and if \( s \) is prime.

Unlike \( T_s \), \( \hat{T}_s \) acts like a binary filtering operator that blocks composite inputs while it allows prime inputs to pass-through without distortion, i.e., performs as a lossless passthrough prime filter with a gain of 1.

Expressions (A2) and (A3) can be coded to programmatically generate \( \pi(s) \) for any \( s > 3 \). A difference between the expressions for \( \pi(s) \) in ([8], p. 593), [11,15], and (A2), (A3) is that we can use the latter to detect primes by obtaining analytically smooth approximations of \( \pi(s) \), theoretically of arbitrary numerical accuracy, through smooth approximations of \( \lfloor \cdot \rfloor \) and \( \delta(\cdot) \). For the integer-part operation \( \lfloor \cdot \rfloor \), we may use Fourier series approximations of the shifted Heaviside step function, while the discrete delta function \( \delta(\cdot) \) may be approximated via a zero-mean normal distribution. While these approximations inevitably introduce numerical errors, in certain special cases we may determine upper bounds for them.

Given that primes occur at the “spikes” of the otherwise flat-line (zero value) graph of the first derivative of \( \pi(s) \), exploring how well we can “detect” the presence of primes as “bumps” in the derivative of a smooth approximation of \( \pi(s) \) might also be a viable path in computational prime number detection.

We may also use (A4) to express GC in algebraic form, for any even \( s \geq 6 \), by writing

\[
G(s) = \delta \left( \prod_{i=2}^{\lfloor s/2 \rfloor} ((s/i) - \lfloor s/i \rfloor) \right)
\]  

(A5)

since \( G(x) \) is 0 if \( x \) is prime and 1 otherwise, so that Goldbach’s conjecture stating that “there always exist two odd primes adding up to \( s \)” is algebraically equivalent to \( D = 0 \) where

\[
D = \prod_{i=3}^{\lfloor s/2 \rfloor} [G(i) + G(s-i)]
\]

**Appendix B. Efficient Searches for Prime-Prime (P-P) Type Pairs within a Partition**

Consider a partition similar to the one discussed in Section 3, for an even \( s \geq 6 \) and no apriori knowledge of any primes in \([1, s-1]\). Since all primes \( > 3 \) are of the form \( 6k \pm 1 \), we can formulate our P-P pair search using modulo algebra in compact notation, as follows:

\[
s = 6k + \{0, 2, 4\} = 6k + \{0, \pm 2\}
\]  

(A6)

\[
s = q_L + p_R
\]  

(A7)

\[
q_L = \{1, 3, 6k \pm 1\}
\]  

(A8)

\[
p_R = 6k \pm 1
\]  

(A9)
where \( k \geq 1 \) is a generic integer constant. From (A7) it follows that \( q_L \) and \( p_R \) are of the form

\[
q_L = \frac{s}{2} - f \quad \text{(A10)}
\]

\[
p_R = \frac{s}{2} + f \quad \text{(A11)}
\]

where \( f \in [0, (s/2) - 1] \) is the partition-generating offset. Instead of using (A8) and (A9) to generate the candidate \( P-P \) pairs, we use (A10) and (A11) based on the admissible values of offset \( f \). We proceed on a case-by-case basis, next.

First, consider the case

\[
s = 6k, \; q_L = 6k + 1
\]

which implies \( s/2 = 3k \). From the above expressions and (A10) we obtain

\[
6k + 1 = 3k - f \quad \text{(A12)}
\]

or equivalently

\[
f = 3\lambda - 1 \quad \text{(A13)}
\]

for \( \lambda \geq 0 \), which gives the admissible values for the offset \( f \) in this case. If \( s/2 \) is even, given that \( q_L \in P_o \) and is therefore odd, it follows from (A10) that \( f \) is odd so that, from (A13), we conclude that \( \lambda \) is even.

Proceeding in a similar manner, we consider the case

\[
s = 6k, \; q_L = 6k - 1, \; s/2 \; \text{even}
\]

and conclude that

\[
f = 3\lambda + 1 \quad \text{(A14)}
\]

where \( \lambda \) is even. Table A1 summarizes the admissible offset values in each case:

| \( s/2 \) | \( s \mod 6 = 0 \) | \( s \mod 6 = 2 \) | \( s \mod 6 = 4 \) |
|---|---|---|---|
| even | \( f = 3\lambda \pm 1, \lambda \geq 0 \; \text{even} \) | \( f = 3\lambda, \lambda \geq 1 \; \text{odd} \) \( f = s/2 - 3 \) | \( f = 3\lambda, \lambda \geq 1 \; \text{odd} \) \( f = s/2 - 3 \) |
| odd | \( f = 3\lambda \pm 1, \lambda \geq 0 \; \text{odd} \) | \( f = 3\lambda, \lambda \geq 0 \; \text{even} \) | \( f = 3\lambda, \lambda \geq 0 \; \text{even} \) \( f = s/2 - 3 \) |

By using (A10) and (A11) and from Table A1, the search for pairs \( (q_L, p_R) \) with \( q_L \in P_o \) and \( p_R \in P_o \) is computationally more efficient, even in the absence of any information about primes in \([1, s]\). If such information is available, we may use it to eliminate additional non \( P-P \) pairs.

From (A10) and (A11), after multiplication, we have that

\[
q_L \cdot p_R = \left(\frac{s}{2}\right)^2 - f^2 \quad \text{(A15)}
\]

which implies that for any \( s \), the product of the summands attains its minimum when \( f = f_{\text{max}} \), i.e., when the distance of \( q_L, p_R \) from the midpoint \( s/2 \) is maximized. Therefore, the prime summand product (PSP) is minimized (maximized) for the \( P-P \) pair with the largest (smallest) distance from the midpoint.

**Appendix C. On the Relative Density of Primes between \([1, x]\) and \([x, 2x]\)**

In Section 3 we established the summative optimality of primes and discussed how this property manifests itself in the partitioning of an even number \( s \). We mentioned how this powerful property is amplified if we consider that the density of primes \( \pi(x)/x \)
decreases as the value of $x$ increases. For larger values of $x$, we might expect to find fewer primes in the second half interval $[x, 2x]$ than the first $[1, x]$ and so we examine the ratio $R(x)$ of primes in $[x, 2x]$ to those in $[1, 2x]$. Using the prime counting function $\pi(x)$ we may write $R(x)$ as

$$R(x) = \frac{\pi(2x) - \pi(x)}{\pi(2x)} = 1 - \frac{\pi(x)}{\pi(2x)}$$

Figure A1 below shows that, as $x \to 3000$, $R(x)$ trends towards 45%, i.e., there is a 10-point (45–55%) split in the prime density values between the two half-intervals. Asymptotically, $\pi(x) \sim x / \log(x)$ ([8], p. 463), so that $\pi(x) / \pi(2x) \sim \log(2x) / [2 \log(x)] \sim 1/2$, implying that $R(x)$ converges to 50% as $x \to \infty$.

![Graph of R(x) = 1 − \pi(x)/\pi(2x).](image)

**Figure A1.** Graph of $R(x) = 1 - \pi(x)/\pi(2x)$.

Convergence, however, is slow: even for much larger values of $x$, the distribution of primes in the two half intervals remains measurably different. Consider, for example, the case $\pi(10^{16}) = 279,238,341,033,925$ and $\pi(2 \cdot 10^{16}) = 547,863,431,950,008$, documented in [16], so that $\pi(10^{16}) / \pi(2 \cdot 10^{16}) \approx 50.9686\%$, or equivalently, $R(10^{16}) = 49.0314\%$, which implies a difference of approximately 10.6 M in the number of primes found between $[1, 10^{16}]$ and $[10^{16}, 2 \cdot 10^{16}]$, or about 1.94% of $\pi(2 \cdot 10^{16})$.

**References**

1. Aristotle. *Metaphysics*; Book 1 sec. 985b–986a, Perseus Digital Library; Tufts University, Massachusetts, USA: Translated in English by Hugh Tredennick: "they (ref. to the Pythagoreans) assumed the elements of numbers to be the elements of everything, and the whole universe to be a proportion (‘Harmony’) or number” and in the Original Greek Text: "τα των ἀριθμῶν στοιχεία τῶν ἄντων στοιχεία πάντων υπέλαβον εἶναι, καὶ τὸν ἄλλον ὀμολογοῦσαν ἀριθμοῦν εἶναι καὶ ἀριθμοῦν." Available online: [http://data.perseus.org/citations/urn:cts:greekLit:tlg0086.tlg025.perseus-eng1:1.985b](http://data.perseus.org/citations/urn:cts:greekLit:tlg0086.tlg025.perseus-eng1:1.985b) (accessed on 29 November 2021).

2. Laertius, D. *Lives of Eminent Philosophers*; Henderson, J., Ed.; Hicks, R.D., Translator; LOEB Classical Library Series; Harvard University Press: Cambridge, MA, USA, 2005; Volume II, pp. 340–347.

3. Guthrie, K. *The Pythagorean Sourcebook and Library*; Alexandria Books; Phanes Press: Grand Rapids, MI, USA, 1988; pp. 299–305, 321–331.

4. Lakš, A.; Most, G. *Early Greek Philosophy*; LOEB Classical Library Series; Fragment D50 (B54) “Invisible Harmony, Stronger Than a Visible One”; and in the Original Greek Text: "αἱρεσία ἀριθμοῦς ὑπερείσις κρείττον."; Harvard University Press: Cambridge MA, USA, 2016; Volume III, p. 162.

5. Euclid. *Elements*, Propositions 7.32 (p. 219) and 9.20 (p. 271) from the Greek Text of J. L. Heiberg (1883–1885) based on *Euclidis Elementa*, Edited and Translated in English by Richard Fitzpatrick. Available online: [http://farside.ph.utexas.edu/Books/Euclid/Elements.pdf](http://farside.ph.utexas.edu/Books/Euclid/Elements.pdf) (accessed on 29 November 2021).

6. Hawking, S. *God Created the Integers*; Propositions 7.32 (p. 92) and 9.20 (p. 101); Running Press: Philadelphia, PA, USA, 2005.

7. Derbyshire, J. *Prime Obsession*; Plume: Washington, DC, USA, 2004; pp. 99–101.

8. Hardy, G.H.; Wright, E.M. *An Introduction to the Theory of Numbers*, 6th ed.; Oxford University Press: New York, NY, USA, 2008; p. 23.
9. Rivest, R.L.; Shamir, A.; Adleman, L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Commun. ACM* 1978, 21, 120–126. Available online: http://people.csail.mit.edu/rivest/Rsapaper.pdf (accessed on 29 November 2021). [CrossRef]

10. Chaitin, G. *Meta Math! The Quest for Omega*; Vintage Books: New York, NY, USA, 2006; pp. 13–22.

11. Wikipedia. Goldbach’s Conjecture. Available online: https://en.wikipedia.org/wiki/Goldbach%27s_conjecture (accessed on 29 November 2021).

12. Caldwell, K. The Prime Pages: Prime Conjectures and Open Questions. Available online: https://primes.utm.edu/notes/conjectures/ (accessed on 29 November 2021).

13. Oliveira e Silva, T.; Herzog, S.; Pardi, S. Empirical verification of the even Goldbach conjecture and computation of prime gaps up to $4 \times 10^{18}$. *Math. Comput.* 2014, 83, 2033–2060. Available online: https://www.ams.org/journals/mcom/2014-83-288/S0025-5718-2013-02787-1/S0025-5718-2013-02787-1.pdf (accessed on 29 November 2021). [CrossRef]

14. Caldwell, K. The Prime Pages: Goldbach’s Conjecture. Available online: https://primes.utm.edu/glossary/page.php?sort=GoldbachConjecture (accessed on 29 November 2021).

15. Weisstein, E.W. Prime Counting Function. MathWorld—A Wolfram Web Resource. Available online: https://mathworld.wolfram.com/PrimeCountingFunction.html (accessed on 29 November 2021).

16. Gourdon, X.; Sebah, P. Numbers, Constants and Computation. Available online: http://numbers.computation.free.fr/Constants/Primes/pixtable.html (accessed on 29 November 2021).