Mathematics and Computer Science
2024, Vol. 9, No. 3, pp. 57-63
https://doi.org/10.11648/j.mcs.20240903.12

Research Article

Representation and Generation of Prime and Coprime Numbers by Using Structured Algebraic Sums

Ioannis Papadakis*

Independent Researcher, Charlotte, USA

Abstract

The algebraic structure and distribution of prime numbers remain two of the most fundamental problems in mathematics. The Fundamental Theorem of Arithmetic, proved by Euclid, and Goldbach's conjecture, while universal in scope with respect to how numbers can be represented multiplicatively or additively, do not provide insights into the structure of primes. Similarly, the definition of a prime −as a number divisible only by 1 and itself− or a sieve algorithm, commonly used to generate primes by successively eliminating multiples, offer no insight into the structure of primes. The powerful and persistent consideration of prime numbers as universal "arithmetic quanta" has not necessitated an equally powerful need for parallel research into a deeper and possibly more insightful explanation of primeness, that is, a better understanding of "why" a number is prime. In this paper, prime and coprime numbers are represented and generated by algebraic expressions. Specifically, given the first n primes, p_1, p_2,…, p_n, sufficient conditions are given for expressing primes greater than p_n, and coprimes with prime factors greater than p_n, as algebraic functions of p_1, p_2,…, p_n. Thus, primality and co-primality are shown to be mathematical properties with inherently evolutionary algebraic characteristics, since larger primes and coprimes can be generated algebraically from smaller ones. The methodology described in the paper can be a useful tool in the study and analysis of the complexity, structure, interrelationships and distribution of primes and coprimes.

Keywords

Prime Number, Prime Factor, Factorization, Coprime, Algebraic Representation, Prime Generation, Coprime Generation, Optimization

1. Introduction

The Fundamental Theorem of Arithmetic (FTA), proved by Euclid (300 BCE), states that any integer greater than 1 can be expressed as a prime, or unique product of primes called prime factors [1, 2]. Goldbach's conjecture, in its broadest interpretation, states that any integer greater than 1 may be expressed as a sum of at most three primes, thus representing a "summative counterpart" to the factorization result of the FTA [3-6].

Such universally optimal representations, multiplicative or summative, do not help us gain meaningful insights into the structure of primes, since, by definition, primes are the "quanta", i.e. indivisible building blocks, of all numbers. For that reason, the primality of a number is typically established, or refuted, by reverting to the definition of a prime: a number that is divisible only by itself and 1. No additional insight into the algebraic structure of primes is gained by applying a sieve:

*Corresponding author: ypap@primactaglobal.com (Ioannis Papadakis)

Received: 11 July 2024; **Accepted:** 29 July 2024; **Published:** 15 August 2024

the set of primes, *P*, corresponds to the "leftover" numbers, i.e. those not eliminated by the sieve algorithm [7]. However, the underlying mathematical structure of primes and coprimes is intrinsic and interdependent, and thus merits a more systematic focus.

In this paper, it is shown that, under certain conditions, the primality of a number is dependent to that of smaller primes in an algebraic sense; a similar result holds for certain coprimes. Our findings demonstrate that primality, and co-primality, are properties with evolutionary characteristics, propagating from smaller to larger primes and coprimes. For example, while it is typically claimed that "3 is prime because it can only be divided by itself and 1", this paper offers an alternative explanation: 3 is prime because it equals $2^1 + 1$. Put differently, it can be shown that the quantity represented by $2^b \pm 1$ is prime, if $2^b \pm 1 < 9$. Hence, the primality of 3, 5 and 7 is a direct algebraic consequence of the primality of 2, without the need to apply the definition of a prime number, or rely on a sieve.

A consequence of the above is that 3, 5 and 7 "inherit" their primality from that of 2. The values, and therefore the distribution, of the next 3 primes, is a direct algebraic result of the primality and value of 2, the first prime. This result may be generalized by describing the algebraic structure that represents, and can therefore generate, prime numbers greater than the n^{th} prime, p_n, as discussed in the next section.

Prior research has established the "quantum optimality", multiplicative and additive, of the set *P* of primes, and the existence of sufficient conditions for the algebraic representation of primes using Hybrid Prime Factorization (HPF), i.e. algebraic expressions containing structured sums [8, 9].

Specifically, this paper extends the results of the research [9], by establishing common, less restrictive sufficiency conditions for the algebraic representation of primes and coprimes. Such expressions can find applications in cryptography, where prime factorization and computationally efficient generation of increasingly large primes are used for securely encrypting and decrypting digital information [10, 11].

The methodology presented in this paper can be a useful tool for the study of the evolutionary characteristics of primality, the relational properties of primes, coprimes, and their distribution.

2. Generation of Primes and Coprimes

The Hybrid Prime Factorization (HPF) algebraic structure, defined in the next section, is used to generate larger primes and coprimes. It consists of a coprime sum or difference, subject to several conditions.

2.1. The HPF Algebraic Structure

"HPF" refers to an algebraic expression of the form

$$\mathrm{HPF} = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_n^{a_n} \pm p_1^{b_1} \cdot p_2^{b_2} \cdot \ldots \cdot p_n^{b_n} \tag{1}$$

where $p_1, p_2 \ldots, p_n$ denote the first n primes and the integer exponents a_i, b_i satisfy the conditions:

$$a_i, b_i \geq 0 \tag{2}$$

$$a_i \cdot b_i = 0 \tag{3}$$

$$a_i + b_i \geq 1 \tag{4}$$

$$\sum_{i=1}^{n} a_i \geq 1 \tag{5}$$

$$\sum_{i=1}^{n} b_i \geq 1 \tag{6}$$

$$\mathrm{HPF} > 1 \tag{7}$$

for $i = 1, 2, 3, \ldots, n$.

Inequalities (2)-(4) ensure that the two multiplicative terms in (1) are coprime, i.e. no p_i can be a factor in both terms, and (5)-(6) prevent either term in (1) to be 1. Condition (7) eliminates any trivial, non-prime solutions, i.e. where $\mathrm{HPF} = 1$, such as: $2^4 - 3 \cdot 5$, $5^2 - 2^3 \cdot 3$, $2^2 \cdot 3^2 - 5 \cdot 7$.

Given the HPF structure (1)-(7), the prime generation result reported in research [9], can be summarized by stating that if

$$\mathrm{HPF} < p_{n+1}^2 \tag{8}$$

then the HPF represents a prime $> p_n$.

Example 1. Let $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$. Each of the HPF expressions below, satisfies (2)-(8) for $n = 3$, and therefore it represents a prime > 5

$$3 \cdot 5 - 2 = 13 \tag{9}$$

$$3 \cdot 5 + 2 = 17 \tag{10}$$

$$2^2 \cdot 3 - 5 = 7 \tag{11}$$

$$2^2 \cdot 3 + 5 = 17 \tag{12}$$

$$2^2 \cdot 3^2 - 5^2 = 11. \tag{13}$$

If the sufficiency conditions (2)-(8) are not satisfied, HPF may or may not be a prime, as shown by the expressions below:

$$2^2 \cdot 3^2 + 5^2 = 61 \text{ is prime; (8) not satisfied} \tag{14}$$

$$2^1 \cdot 3^3 - 5 = 49 \text{ is not prime; (8) not satisfied} \tag{15}$$

$$2^2 + 5^2 = 29 \text{ is prime; (4) not satisfied} \tag{16}$$

$$2^6 - 5 = 59 \text{ is prime; (4) and (8) not satisfied.} \tag{17}$$

The result described in the above example can be generalized, based on the observation that when the HPF satisfies (2)-(7) but not (8), it will either be a prime ≥ 7, or a compo-

site number, coprime to $\{2, 3, 5\}$, with at most k prime factor terms, where k is the smallest integer such that $HPF < 7^{k+1}$. Hence, the prime generation result reported in research [9], corresponds to the special case $k = 1$, for which the HPF value is predictably prime. The following proposition formalizes this generalized result.

Proposition 1. The HPF expression, given by (1), subject to (2)-(4) and (7), is:

(i) co-prime to $p_1, p_2 \ldots, p_n$;

(ii) $HPF \geq p_{n+1}$;

(iii) the number of terms in the prime factorization of the HPF is at most k, where $k \geq 1$ is such that

$$k \leq \frac{\log(HPF)}{\log(p_{n+1})} < k + 1 \tag{18}$$

and $\log(\cdot)$ denotes the natural logarithm function.

Proof. The HPF, given by (1), cannot have any of $p_1, p_2 \ldots, p_n$ as prime factor(s), since this would lead to a contradiction, given that the two product terms in (1) are coprime, by virtue of conditions (2)-(4) and (7). Hence, $HPF > 1$ is coprime to $p_1, p_2 \ldots, p_n$, which proves the first part of the proposition. From this, it follows that the minimum value of the HPF is p_{n+1}, i.e. its smallest prime factor. Therefore

$$HPF \geq p_{n+1}. \tag{19}$$

To prove the last part of the proposition, let $k \geq 1$ such that

$$p_{n+1}^k \leq HPF < p_{n+1}^{k+1}. \tag{20}$$

Since every prime factor of HPF is $\geq p_{n+1}$, it follows that the HPF cannot have more than k terms in its prime factorization, since this would violate the right side of (20). By taking the natural logarithms of all sides of (20), expression (18) follows, and the last part of the proposition is proved.

From Proposition 1, it follows that for the special case $k = 1$, the HPF, given by (1), is a prime number in the semi-open interval $[p_{n+1}, p_{n+1}^2)$. For higher values of k, the HPF is either a prime or coprime in the semi-open interval $[p_{n+1}^k, p_{n+1}^{k+1})$, with a maximum "prime factor cardinality" of k, i.e. having at most k terms in its prime factorization (including any repeating primes).

The following examples show how Proposition 1 can be used to represent, and thus generate, primes and coprimes.

Example 2. Let $n = 3$ and consider the HPF expression (15) of the previous example. In this case, $k = 2$, since

$$HPF = 2^1 \cdot 3^3 - 5 = 49 = p_4^2 \tag{21}$$

and HPF is coprime to $\{2, 3, 5\}$, with a maximum prime factor cardinality of 2 and no prime factor smaller than 7.

Example 3. Consider the HPF expression ($n = 3$), given by

$$HPF = 2^{10} \cdot 3^5 \cdot 5^5 + 1 = 777{,}600{,}001 \tag{22}$$

for which, the corresponding value of k, from (18), is

$$k = \left\lfloor \frac{\log(HPF)}{\log(p_4)} \right\rfloor = \left\lfloor \frac{\log(777{,}600{,}001)}{\log(7)} \right\rfloor = 10 \tag{23}$$

where $\lfloor \cdot \rfloor$ denotes the integer part operator. The above equation implies that (22) has a maximum prime factor cardinality of 10, with no prime factor < 7. This is confirmed by the prime factorization of the HPF, given by

$$HPF = 777{,}600{,}001 = 31 \cdot 61 \cdot 411{,}211. \tag{24}$$

The value of the HPF expression (1) may be minimized with respect to the exponents a_i, b_i, subject to the conditions of Proposition 1, to maximize the likelihood of the HPF representing a relatively smaller prime $> p_n$, or a (composite) coprime $> p_n$ with relatively small prime factors and cardinality.

In general, (1) may be viewed as an algebraic generator of primes and coprimes. Its prime and coprime generating performance is analyzed in Section 3.

2.2. Evolutional Characteristics of Primality

The algebraic system described by (1)-(4) and (7) lends itself to a hierarchical evolutionary structure in the generation of primes from smaller ones. The relaxation of conditions (5)-(6) implies that such hierarchical generation can be traced to the smallest possible prime. To show this, consider a, where $a = 1 + 1$. Since $1 < a < 4$, with 4 being the smallest possible non-prime (composite) number, it follows that 2 and 3 are prime. The primality of 3 may also be established from the primality of $HPF = 2^2 - 1$, since it represents a number > 2 and < 4.

The primality of $HPF = 2^2 + 1$ and $HPF = 2^3 - 1$ also follows directly from that of 2, i.e. without relying on the primality of $p_2 = 3$. Since $HPF = 2^b \pm 1$, for $b > 1$, satisfies (1)-(4) and (7), and $p_2 \geq 3$, it follows that a lower bound of p_2^2 is 9, i.e. $3^2 \leq p_2^2$. From Proposition 1, every value of this HPF within the interval $[1,9)$ is, a priori, prime. Hence, the expressions $2^2 + 1$ and $2^3 - 1$ represent primes.

For $n = 1$, since 7 cannot be generated by an expression of the form $2^b + 1$, it follows that some primes may be represented by an HPF sum or a difference, not both. For $n = 2$, the number 7 can be represented by the HPF sum: $2^2 + 3^1$.

Violation of condition (20), for $k = 1$, i.e. if $HPF \geq 3^2$, neither guarantees nor precludes the primality of $HPF = 2^b \pm 1$. For example: $2^4 + 1$ and $2^5 - 1$ are both prime, but $2^3 + 1$ and $2^4 - 1$ are not.

3. Prime Generator Performance

In this section, the performance of the system (1), (2)-(4) and (7), viewed as a algebraic prime number generator, is evaluated theoretically and by using Monte Carlo simulation.

3.1. Definitions and Measures of Performance

From Proposition 1, the expression (1), subject to (2)-(4), (7), either generates a prime $> p_n$, or a coprime to $p_1, p_2 \ldots, p_n$, with at most k terms in its prime factorization, where

$$k = \left\lfloor \frac{\log(HPF)}{\log(p_{n+1})} \right\rfloor. \quad (25)$$

As discussed in the previous section, the special case, $k = 1$, implies that

$$HPF < p_{n+1}^2 \quad (26)$$

and thus, the HPF, given by (1), is a prime number in the semi-open interval $[p_{n+1}, p_{n+1}^2)$. To facilitate the analysis of the "prime generating" performance of (1), its "prime generating power", $P(n,k)$, is defined as a measure of how likely it is for (1) to generate a prime.

Definition 1. The "prime generating power", $P(n,k)$, of an HPF, given by (1), subject to (2)-(4) and (7), is defined by

$$P(n,k) = \frac{\text{Number of HPF primes in } [p_{n+1}^k, p_{n+1}^{k+1})}{\text{Number of HPF outcomes in } [p_{n+1}^k, p_{n+1}^{k+1})}. \quad (27)$$

From the above definition, it follows that $P(n,k) \leq 1$. The quantity $P(n,k)$ expresses the likelihood that (1) generates a prime number within a given value range. Next, it is shown that $P(n,k)$ starts at 100% for $k = 1$ and decreases as the value of k increases.

Corollary 1. For any $n \geq 1$: $P(n,1) = 1$, and $P(n,k) < 1$ for $k \geq 2$.

Proof. If $k = 1$, from Proposition 1 and (20), it follows that (26) is true. Since the smallest non-prime having all its prime factors greater than p_n is equal to p_{n+1}^2, the HPF expression, given by (1), will always generate a prime number in $[p_{n+1}, p_{n+1}^2)$. Therefore, the numerator and denominator in (27) are equal, and thus $P(n,1) = 1$. For higher values of k, the HPF can take non-prime values, and therefore $P(n,k) < 1$.

Proposition 1 implies that, within the value range $[p_{n+1}, p_{n+1}^2)$, expression (1), subject to (2)-(4), (7) generates a prime number with certainty, i.e. $P(n,1) = 100\%$. In the general case, i.e. for HPF values $\geq p_{n+1}^2$, this percentage is < 1, i.e. the value of $P(n,k)$ decreases as k increases, as described in Proposition 1. The variation of $P(n,k)$ with respect to changes in the values of n and k is analyzed in the next section.

It is infeasible to exhaustively determine all possible HPF values in a given interval, since it cannot be precluded that, for some higher exponent values, the difference in (1) would not generate a relatively small prime. Consider, for example, the following HPF, where $n = 6$, given by

$$HPF = 5^1 \cdot 13^3 - 2^4 \cdot 3^2 \cdot 7^1 \cdot 11^1$$

or

$$HPF = 10985 - 11088 = 103 \quad (28)$$

represents a prime, since $HPF < p_7^2$, where $p_7 = 17$. The two coprime terms in (28) are, approximately, 100 times greater than the value of the HPF. Hence, it is possible to generate primes in $[p_{n+1}, p_{n+1}^2)$ by subtracting coprime terms that are several orders of magnitude greater.

Under the assumption that (1) can generate every prime and coprime, it follows that evaluating its actual performance, given by $P(n,k)$, is equivalent to assessing its predicted performance, $\hat{P}(n,k)$, defined below.

Definition 2. The "predicted prime generating power", $\hat{P}(n,k)$, of an HPF, given by (1), subject to (2)-(4) and (7), is defined by

$$\hat{P}(n,k) = \frac{A(n,k)}{A(n,k)+B(n,k)} \quad (29)$$

where $A(n,k)$ is the number of primes in $[p_{n+1}^k, p_{n+1}^{k+1})$, and $B(n,k)$ is the number of composites in $[p_{n+1}^k, p_{n+1}^{k+1})$, coprime to $p_1, p_2 \ldots, p_n$.

As previously mentioned, $\hat{P}(n,k)$ is useful for two reasons:

(i) the computational complexity of computing all the solutions of (1), subject to (2)-(4) and (7), for $n \geq 10$ easily exceeds the computational capabilities of a typical computer system, since the two terms comprising the difference in the HPF expression, given by (1), can reach extremely large values, even before generating an HPF prime within the desired range.

(ii) it is not known if every such prime and coprime can be represented by at least one solution in the form of (1).

In the next section, the theoretically predicted $\hat{P}(n,k)$ and the actual $P(n,k)$, obtained by Monte Carlo simulation, are computed and compared.

3.2. Predicted vs. Simulated Performance

Since $B(n,k) = 0$ for $k = 1$, it follows that $\hat{P}(n,1) = 100\%$, for any HPF value in $[p_{n+1}, p_{n+1}^2)$. Therefore, a single value is assigned to $\hat{P}(n,k)$ within each interval $[p_{n+1}^k, p_{n+1}^{k+1})$, starting with $\hat{P}(n,1) = 1$ for $k = 1$. For a range of n,k values, the number of primes and coprimes within each interval $[p_{n+1}^k, p_{n+1}^{k+1})$ is computed, and the corresponding value of $\hat{P}(n,k)$ for that interval is evaluated.

To avoid the time-consuming component of performing prime factorization for each HPF value, the computation of $A(n,k)$, $B(n,k)$ and $\hat{P}(n,k)$, utilizes the list of the first 1M primes from [12]. The results are summarized in the following table.

Table 1. *Predicted performance,* $\hat{P}(n,k)$, *for* $n = 3,4,5$ *and* $k = 1,\ldots,5$.

k	n = 3	n = 4	n = 5	Average
1	100%	100%	100%	100%
2	63.6%	67.9%	67.5%	66.4%
3	50.3%	52.6%	49.2%	50.7%
4	39.7%	41.2%	39.0%	40.0%
5	33.0%	34.1%	32.1%	33.1%

From Table 1, the values of $\hat{P}(n,k)$ do not vary significantly for $n = 3,4,5$. This observation has an interesting practical implication when searching for primes in higher order intervals, i.e. $[p_{n+1}^{k}, p_{n+1}^{k+1})$ for $k > 1$: it implies that the likelihood that HPF is prime does not change significantly as n increases. The last column of Table 1 shows the average values for each k.

The above values of $\hat{P}(n,k)$ are compared to $P(n,k)$, obtained by Monte Carlo simulation. To avoid runtime overflow errors, all exponent parameters in (1) are capped. The Monte Carlo simulation results are summarized in Table 2.

Table 2. *Simulated performance,* $P(n,k)$, *for* $n = 3,4,5$, *and* $k = 1,\ldots,5$.

k	n = 3	n = 4	n = 5	Average
1	100.0%	100.0%	100.0%	100.0%
2	66.7%	65.7%	65.6%	66.0%
3	52.4%	47.3%	50.9%	50.2%
4	38.3%	42.7%	37.6%	39.5%
5	29.4%	33.1%	32.9%	31.8%

From Tables 1 and 2, it follows that:

(i) The average prime-generation performance of the HPF Prime and Coprime Generator (HPF PCG for short) is 50% or higher within the HPF range $[p_{n+1}, p_{n+1}^{4})$, i.e. for $k \leq 3$.

(ii) When the HPF PCG generates a coprime number q, the value of k from (18) can be used to determine the maximum number of terms in the prime factorization of q. This can be used to eliminate a significant number of prime factor combinations that do not generate a product with the same last digit as q, making the prime factorization of HPF PCG coprimes more computationally efficient. This point is illustrated in Example 4.

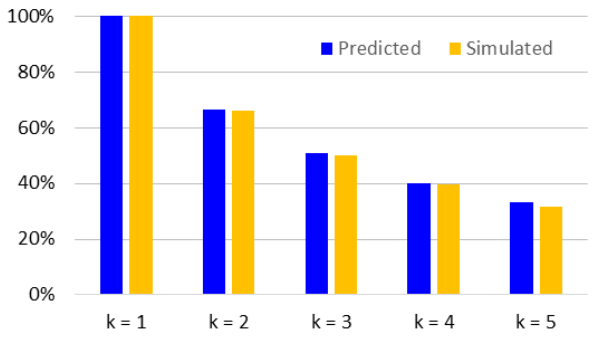

Figure 1. *Comparison of average predicted vs. simulated HPF prime-generation performance, for* $k = 1,\ldots,5$.

The results in Tables 1 and 2 are shown graphically in Figure 1. The average values of predicted performance, $\hat{P}(n,k)$, and simulated performance, $P(n,k)$, are not significantly different for $k = 1,\ldots,5$.

Example 4. For $n = 4$, the HPF given by

$$\text{HPF} = 2^1 \cdot 5^4 + 3^2 \cdot 7^1 = 1250 + 63 = 1313$$

or

$$\text{HPF} = 13 \cdot 101 \tag{30}$$

generates a coprime number. Applying (18), it follows that $k = 2$. Therefore, the prime factorization of 1313 has at most 2 terms, i.e. a maximum prime factor cardinality of 2, and since HPF is coprime, it follows that HPF has exactly 2 prime factors.

Let p and q be primes, such that

$$p \cdot q = 1313. \tag{31}$$

Since p, q can only end in 1, 3, 7 or 9, for their product to end in 3, there can only be four last-digit combinations: (1,3), (3,1), (7,9), (9,7). Also, since $\min(p,q) \geq 11$, it follows that $\max(p,q) \leq 119$. From Proposition 1, it follows that HPF is coprime to the first 4 primes. Thus, it is only necessary to test if HPF is divisible by an odd number w, where $w \in [11,119]$, and $w \bmod 10 = 1$ or $w \bmod 10 = 7$, i.e. a total of 44 possible numbers. This subset of possible factors may be further reduced, from 44 to 26, by excluding multiples of 3 or 7, e.g. 21, 27, 33, 39, 49 etc., generating an additional reduction of 41%. The remaining values are coprime with respect to the first 4 primes, and since $w < 11^2$, they are prime. The unique prime factorization solution is easily determined to be $p = 13$ and $q = 101$. This process significantly reduces the potential number of prime factors of an HPF-generated coprime, thus increasing computational efficiency. In general, the factorization of any HPF-generated coprime results in the determination of at least two primes greater than p_n.

As discussed in the previous example, the increased computational efficiency in searching for prime factors of

HPF-generated coprimes is a result of the a priori knowledge of their maximum prime factor cardinality, established by Proposition 1 (part 3). In general, the computational savings in the prime factorization of an HPF coprime in $[p_{n+1}^{k}, p_{n+1}^{k+1})$, generated by (1), subject to (2)-(4) and (7), are twofold:

(i) none of the n primes $p_1, p_2 \ldots, p_n$ should be considered, since they are not prime factors of any HPF coprime, and

(ii) since the prime factor cardinality of the HPF coprime is at most equal to k, where k is given by (18), the subset of admissible prime factors, for each cardinality scenario, is reduced by considering only those candidate primes whose product ends in the same digit as the HPF coprime. Moreover, for each cardinality scenario, upper and lower bounds for the prime factors of the HPF can be derived, as discussed below.

Consider the case where the total prime factor cardinality of the HPF coprime equals m, where $m \in [2, k]$. It then follows that the upper and lower bounds for each prime factor $q_j > p_n$, of the HPF, are given by

$$HPF = \prod_{j=1}^{m} q_j \tag{32}$$

$$p_{n+1} \le \min_j(q_j) \le \left\lfloor \sqrt[m]{HPF} \right\rfloor \tag{33}$$

$$\max_j(q_j) \le \left\lfloor \frac{HPF}{p_{n+1}^{m-1}} \right\rfloor. \tag{34}$$

Given that total prime factor cardinality includes any repeating prime factors, as explained in Section 2.1, (32) does not imply that the q_j, $j = 1, \ldots, m$, are different. For example, if $HPF = 13^4$, then $m = 4$ and $q_j = 13$, for $j = 1, \ldots, 4$.

Some of the computational efficiencies, described above, materialize even when the lower bound, $p_n + 2$, is used, instead of p_{n+1}. Given that $p_n < p_n + 2 \le p_{n+1}$, it follows that no HPF prime factor is less than $p_n + 2$. Since there are at most k* prime factors, where k^* is given by

$$k^* = \left\lfloor \frac{\log(HPF)}{\log(p_n+2)} \right\rfloor \tag{35}$$

the next step is to proceed by considering feasible factors for each cardinality value, up to k^*. Any odds not coprime to $p_1, p_2 \ldots, p_n$, cannot be factors of the HPF coprime, since this would imply that the HPF is not coprime to $p_1, p_2 \ldots, p_n$. If the total prime factor cardinality of the HPF coprime is m, where $m \in [2, k^*]$, the modified upper and lower bounds for each prime factor q_j, are given by:

$$p_n + 2 \le \min_j(q_j) \le \left\lfloor \sqrt[m]{HPF} \right\rfloor \tag{36}$$

$$\max_j(q_j) \le \left\lfloor \frac{HPF}{(p_n+2)^{m-1}} \right\rfloor. \tag{37}$$

As expected, the modified bounds, given by (36)-(37) are weaker than those in (33)-(34), respectively.

Example 5. Consider the factorization of the coprime HPF (n = 4), generated by

$$HPF = 2^4 \cdot 3^3 \cdot 7^2 - 5^3 = 2899 = 13 \cdot 223. \tag{38}$$

Since no prime factor of 2899 is less than 7+2 = 9, it follows that

$$k^* = \left\lfloor \frac{\log(2899)}{\log(9)} \right\rfloor = 3. \tag{39}$$

and the total prime factor cardinality of 2899 is at most 3.

Consider the first case, where the prime factor cardinality, m, is $m = 2$, i.e. 2899 is assumed to be represented by

$$2899 = q_1 \cdot q_2 \tag{40}$$

where q_1, q_2 are prime. It follows, from (36)-(37), that

$$9 \le \min(q_1, q_2) \le 53 \tag{41}$$

$$\max(q_1, q_2) \le 321. \tag{42}$$

From the subset of odd numbers satisfying (41)-(42), only those with compatible last digits need to be considered, i.e. whose product ends in 9. There are 4 possible combinations:

if q_1 ends in 1 then q_2 should end in 9
if q_1 ends in 9 then q_2 should end in 1
if q_1 ends in 3 then q_2 should end in 3
if q_1 ends in 7 then q_2 should end in 7.

Note that #1 and #2 are symmetric, and therefore only one of those should be considered, something that further increases the computational efficiency of the prime factor search. This search yields two factors of 2899, coprime to 2, 3, 5, 7: 13 and 223.

It remains to be established that these factors are prime. Since $13 < 81$, it follows that 13 is smaller than the smallest HPF coprime, therefore 13 is prime. Since the smallest prime factor of 223 cannot exceed $\left\lfloor \sqrt[2]{223} \right\rfloor = 14$, only 11 and 13 need to be considered. Since neither 11 nor 13 are factors, 223 is a prime factor. Given that prime factors are unique, the case m = 3 need not be considered.

4. Conclusions

Primes greater than p_n, for $n \ge 2$, and coprimes with prime factors $> p_n$, can be generated algebraically using the HPF expression given by (1), subject to (2)-(4) and (7). The sufficiency condition (18) gives the maximum total prime factor cardinality of the HPF. For the special case where the cardinality bound, k, equals 1, the HPF is a priori prime, i.e. its primality can be established without computing its numerical value.

In cases where the HPF generates a coprime, the lower and upper bounds on its prime factors, and the upper bound on the total cardinality of its prime factorization (including any prime factors with multiplicity >1) result in additional computational efficiencies in the prime factor search. In addition,

the prime factorization of any HPF coprime yields at least two primes greater than p_n.

The methodology described in this paper may be used to algebraically represent, generate, efficiently compute, factor and analyze larger primes and coprimes. In the case of prime factorization of HPF-generated coprimes, computational efficiencies are realized even when weaker non-prime bounds are used.

The approach described in the paper unifies the structural characteristics of primes and coprimes, using a common algebraic representation. Such an approach can be a useful tool for studying their distribution and interrelationships.

Abbreviations

FTA	Fundamental Theorem of Arithmetic
HPF	Hybrid Prime Factorization
PCG	Prime and Coprime Generator

Author Contributions

Ioannis Papadakis is the sole author. The author read and approved the final manuscript.

Conflicts of Interest

The author declares no conflicts of interest.

References

[1] Euclid, *Elements*, proposition 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 [Online]. Available: https://farside.ph.utexas.edu/Books/Euclid/Elements.pdf

[2] S. Hawking, *God Created the Integers: The mathematical breakthroughs that changed history*; Propositions 7.32 (p. 92) and 9.20 (p. 101); Running Press: Philadelphia, PA, USA, 2005.

[3] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, New York NY, USA: Oxford University Press, 2008 (6^{th} edition), p. 23.

[4] C. K. Caldwell, The Prime Pages: Goldbach's conjecture. [Online]. Available: https://t5k.org/glossary/page.php?sort=GoldbachConjecture

[5] C. K. Caldwell, The Prime Pages: Prime Conjectures and Open Questions. [Online]. Available: https://t5k.org/notes/conjectures/

[6] T. Oliveira e Silva, S. Herzog and S. Pardi, "Empirical verification of the even Goldbach conjecture and computation of prime gaps up to $4 \cdot 10^{18}$", *Mathematics of Computation*, 83 (2014), 2033-2060, November 2013. Available: https://www.ams.org/journals/mcom/2014-83-288/S0025-5718-2013-02787-1/S0025-5718-2013-02787-1.pdf

[7] J. Derbyshire, *Prime Obsession: Bernhard Riemann and the Greatest Unsolved Problem in Mathematics*; Plume: Washington, DC, USA, 2004; pp. 99–101.

[8] I. N. M. Papadakis, On the Universal Encoding Optimality of Primes. Mathematics 2021, 9 (24), 3155. https://doi.org/10.3390/math9243155

[9] I. N. M. Papadakis, Algebraic Representation of Primes by Hybrid Factorization. Math. Comput. Sci. 2024, 9(1), 12-25. https://doi.org/10.11648/j.mcs.20240901.12

[10] R. L. Rivest, A. Shamir, L. Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Commun. ACM 1978, 21, 120–126. Available: http://people.csail.mit.edu/rivest/Rsapaper.pdf

[11] D.-T. Dam, T.-H. Tran, V.-P. Hoang, C.-K. Pham, T.-T. Hoang, A Survey of Post-Quantum Cryptography: Start of a New Race. Cryptography 2023, 7, 40. Available: https://doi.org/10.3390/cryptography7030040

[12] C. K. Caldwell, The Prime Pages: The first fifty million primes. Available: https://t5k.org/lists/small/millions/