Abstract

Associate a unique numerical sequence called the modular signature with each positive integer, using modular residues of each integer under the prime numbers, and distinguishing between the “core seed primes” and “non-core seed primes” used to create the modular signatures. Group the modular signatures within primorials. Use elementary sieve properties and combinatorial principles to prove the twin primes conjecture.

Introduction

The twin primes conjecture arose from an open question about the distribution of prime numbers. The conjecture states the following: There are infinitely many integers n, such that n-1 and n+1 are both prime \([1]\). Stated another way, there are infinitely many pairs of primes whose gap is 2. For example, the twin prime pair 17 and 19 have a gap of 19-17 = 2.

While mathematicians have found many patterns in the prime numbers, they have continued to pursue proofs of the twin primes conjecture. Neale has described the efforts in the last decade to reduce the size of the twin primes gap to 6, conditioned on the truth of the generalized Elliott-Halberstam Conjecture \([2]\).

Our approach will be to examine residue cycles under congruence classes using combinatorial theory.

Part 1: Foundation

The Sieve of Eratosthenes

Eratosthenes (276-194 B.C.), born approximately 50 years after Euclid, was a contemporary of Archimedes. He created a sieve method to generate all prime numbers less than or equal to a given integer value \(N\). Starting with 2, all integer multiples of 2 are struck from the list up to \(N\); then the remaining multiples of 3 are removed, then the remaining multiples of 5 (4 being skipped since it is a multiple of 2), etc. The result is that once the multiples of the largest prime less than the square root of \(N\) have been eliminated in the sieve, there are no more values to be struck from the list, and what remains are all of the primes less than or equal to \(N\). \([3]\)

Definition: Let \(N\) be a positive integer greater than or equal to 4. Then the set of seed primes in \(N\) equals the set of primes less than or equal to the square root of \(N\).

For example, if \(N = 210\) and the \(\sqrt{N} = 14.49\), then the set of seed primes \(= \{2, 3, 5, 7, 11, 13\}\), where 13 is the largest prime less than or equal to 14.49.

The following are observations about the sieve of Eratosthenes:

- If \(N\) is the largest integer to be used to determine the elements in the sieve, then the largest prime used to generate the sieve is \(\leq \sqrt{N}\). Let \(P_N\) equal the largest prime less than or equal to \(\sqrt{N}\).
- As \(N\) increases to very large numbers, the ratio \(N / \sqrt{N}\) increases accordingly (though more slowly). Similarly, for \(P_N\) equal to the largest prime \(\leq \sqrt{N}\) the ratio \(N / P_N\) increases to very large numbers as \(N\) increases to very large numbers, as well as for the ratio of \(N\) to each prime less than \(P_N\).
• For primes \( P_r \leq P_N \), as the ratio of \( N / P_r \) increases, it permits more multiples of \( P_r \) to be generated in the sieve. The result is that the increase in the number of primes slows as \( N \) increases while the corresponding increase in the number of composites grows.

• As each prime \( P_r \leq P_N \) generates new composites, its first new composite occurs at \( P_r^2 \) and each subsequent new composite of \( P_r \) is a multiple of \( P_r \) and one or more primes greater than or equal to \( P_r \). Consequently, each \( P_r \) produces fewer new multiples < \( N \) than its predecessor in the sieve.

**Congruence Classes**

If \( S \) is a divisor of \( X - r \), then we say that \( X \) is congruent to \( r \) modulus \( S \), and we write

\[
X \equiv r \text{ Mod } S
\]

and refer to \( r \) as the residue (or remainder) of \( X \) Mod \( S \). If \( 0 \leq r \leq S \), then \( r \) is the least residue of \( X \) Mod \( S \). Further, two numbers, \( X \) and \( Y \), are congruent if they have the same residue under Mod \( S \). That is, if \( X \equiv r \) Mod \( S \) and \( Y \equiv r \) Mod \( S \), then we say that \( X \) and \( Y \) are congruent under Mod \( S \). [4] For example, since \( 47 \equiv 2 \) Mod \( 5 \) and \( 7 \equiv 2 \) Mod \( 5 \), we say that \( 47 \) and \( 7 \) are congruent under Mod \( 5 \) because they have the same modular residue when divided by \( 5 \).

A congruence class Mod \( S \) is the class of all numbers congruent to a given residue Mod \( S \), and every member of the class, denoted by \([r]\), is called a representative of the class. Further, for each \( S \), there are \( S \) classes, represented by the integers \( 0, 1, 2, \ldots S-1 \). For example, for \( S = 5 \), there are five congruence classes: \([0]\), \([1]\), \([2]\), \([3]\) and \([4]\). In our example, \( 47 \) and \( 7 \) are members of congruence class \([2]\) for Mod \( 5 \).

• For each modulo \( P \) where \( P \) is a prime number, congruence class \([0]\) has only one prime number representative: the prime number \( P \) itself. All other members of \([0]\) are multiples of \( P \).

• All integers in class \([1]\) are of the form \( n*P + 1 \), for integers \( n \geq 0 \). Similarly, all integers in \([2]\) are of the form \( n*P + 2 \), for integers \( n \geq 0 \), and so forth for successively higher integers.

• In Mod \( 3 \), the prime numbers > \( 3 \) are in either congruence class \([1]\) or \([2]\). Similarly, under Mod \( 5 \), the prime numbers not equal to \( 5 \) are distributed over the four non-zero congruence classes. In fact, as \( P \) gets bigger, the primes \( \neq P \) are distributed over \( P-1 \) congruence classes (all those \( \neq [0] \)), with the same separation (or gap) as their original differences, mod \( P \) (i.e. \( P_i - P_j \equiv [r_i] - [r_j] \) Mod \( P \)).

• Under de la Vallee Poussin’s Theorem (1896) [5], there are an infinite number of primes in each non-zero congruence class, and as \( P_N \) increases to a large number, each congruence class > \([0]\) Mod \( P \) will have approximately the same number of primes (i.e. \( \frac{\pi(N)}{P(P-1)} \) * \( \pi(N) \), where \( \pi(N) \) equals the number of primes \( \leq N \)). So, for example using Mod \( 3 \), approximately one half of all primes will be in \([1]\) Mod \( 3 \) and one-half in \([2]\) Mod \( 3 \), with only 3 itself in \([0]\) Mod \( 3 \).

**Modular Signatures of the Positive Integers**

Table 1 below shows the “seed primes” (2, 3 and 5) for the even number \( 30 = 2*3*5 \) which the sieve uses to generate the prime values larger than \( 5 \) and less than \( 30 \). The table also shows the “signature” of each integer, consisting of its residues under modular arithmetic for each seed prime, ordered from the smallest seed prime to the largest. Because of the Fundamental Theorem of Arithmetic [6], each positive integer has a unique “signature” of modular residues under all of the prime numbers.

**Definition:** The modular signature of a positive integer, \( Z \), is its unique ordered (on prime numbers \( P_r \) in ascending order starting with 2) sequence of modular residues, \((s_1, s_2, \ldots, s_N)\), under the prime numbers less than or equal to some maximum seed prime, \( P_N \), where

\[
Z \equiv s_i \text{ Mod } P_r \text{ for each } 2 \leq P_r \leq P_N
\]
For example, the modular signature of the positive integer (and prime number) 13 under seed primes up to 19 is: (13 Mod 2, 13 Mod 3, 13 Mod 5, 13 Mod 7, 13 Mod 11, 13 Mod 13, 13 Mod 17, 13 Mod 19) which is equal to this modular signature: (1, 1, 3, 6, 2, 0, 13, 13).

Of particular interest is the fact that the modular residue s, of any integer, Z, equals Z for all seed primes greater than Z. That ensures that the modular signatures of every positive integer will be unique when seed primes are used that are greater than Z. For example, the modular signature of the integer 7 is the sequence (1, 1, 2, 0, 7, 7, 7, 7, 7, 7) under the first ten seed primes 2, 3, 5, 7, 11, 13, 17, 19, 23 and 29.

Table 1 below shows all possible combinations of modular residues for \( E = 30 \), using the factors of 30 (2, 3 and 5) as seed primes, generating a complete cycle of all of the combinations from 1 to 30 of the seed primes’ modular residues.

Table 1

| Integer | 2 | 3 | 5 | Twin Prime |
|---------|---|---|---|------------|
| 1       | 1 | 1 | 1 |             |
| 2       | X | 0 | 2 |             |
| 3       | X | 1 | 0 |             |
| 4       |   | 0 | 1 |             |
| 5       | X | 1 | 2 | X           |
| 6       |   | 0 | 0 |             |
| 7       | X | 1 | 1 | 2           |
| 8       |   | 0 | 2 | 3           |
| 9       |   | 1 | 0 | 4           |
| 10      |   | 0 | 1 |             |
| 11      | X | 1 | 2 | 1           |
| 12      | X | 0 | 0 | 2           |
| 13      | X | 1 | 1 | 3           |
| 14      |   | 0 | 2 | 4           |
| 15      |   | 1 | 0 | 0           |
| 16      |   | 0 | 1 |             |
| 17      | X | 1 | 2 | 2           |
| 18      |   | 0 | 0 | 3           |
| 19      | X | 1 | 1 | 4           |
| 20      |   | 0 | 2 | 0           |
| 21      |   | 1 | 0 | 1           |
| 22      |   | 0 | 1 | 2           |
| 23      | X | 1 | 2 | 3           |
| 24      |   | 0 | 0 | 4           |
| 25      |   | 1 | 1 | 0           |
| 26      |   | 0 | 2 | 1           |
| 27      |   | 1 | 0 | 2           |
| 28      |   | 0 | 1 | 3           |
| 29      | X | 1 | 2 | 4           |
| 30      |   | 0 | 0 | 0           |

Note: Only the larger of the pair is listed for twin primes.

Starting at 31, each of the seed primes 2, 3 and 5 will repeat its residue cycle in the same order for every increment of 30, so obviously more seed primes > 5 are needed to maintain unique modular signatures for integers > 30. Consequently, modular signature for integers > 30 will have to expand to include the modular residue(s) of one or more additional seed primes so as to eliminate the possibility of duplicate signatures. In the next section, we will define the maximum seed prime for all modular signatures used in this paper, with the requirement that the maximum seed prime be large enough to eliminate the possibility of duplicate modular signatures.

**Primorials and Modular Signatures**

The product of consecutive prime numbers starting with 2 and up to a largest prime, \( P \), is called a primorial and is denoted by \( P\# \). [7] In this paper we will use primorials to frame our modular signatures to ensure
that the modular signatures contain enough residue elements to show that they are unique for each positive integer.

Note the following about Table 1 and primorial 30 = 2*3*5:
1. 30 is the only primorial for which its largest seed prime (5) also is the largest prime factor of 30.
2. Since there are two modular residues for seed prime 2, three residues for seed prime 3 and five residues for seed prime 5, there are 2*3*5 = 30 possible combinations of the residues to produce the modular signatures of the integers from 1 to 30. Thus, the seed primes of 30 generate all possible combinations of modular signatures of the residues under seed primes 2, 3 and 5 in primorial 30.
3. The three seed primes of 30 each have modular signatures containing one 0, which is the residue for each respective seed prime when divided by itself. Otherwise, a prime number greater than 5 and less than 30 has no zeros in its modular signature.
4. While there will be other integers greater than a seed prime that may have just one 0 in their modular signature (e.g. the number 25), they are composites because they are the product of more than a single power of the seed prime and the number 1 (e.g. 25 = 5^2 * 1).
5. We can use the following formula to count the number of primes in primorial 30: 3 + [(2-1)*(3-1)*(5-1)] -1 = 10, where 3 equals the number of seed primes, [(2-1)*(3-1)*(5-1)] equals the number of combinations of non-zero residues of the three seed primes and -1 is included to subtract the number 1 from the positive combinations because 1 is not a prime number by definition.

To proceed, then, we will need to have a consistent method for determining the maximum seed prime required to produce the unique modular signature for a positive integer.

Definition: Let N be a positive integer. Then the maximum seed prime for N’s modular signature will be the largest prime less than or equal to the square root of the smallest primorial, E, greater than or equal to N.

For example, if N = 68, then E = 7# = 210 = 2*3*5*7 is the smallest primorial greater than or equal to 68. Since 13 is the largest prime less than \(\sqrt{210}\), the modular signature for 68 will use seed primes 2, 3, 5, 7, 11 and 13, and every positive integer less than primorial 210 (including 68) will have a unique modular signature under the seed primes up to and including 13.

Whereas the Sieve of Eratosthenes uses the \(\sqrt{N}\) to identify the maximum prime that will be used to generate primes less than or equal to a positive integer N, we use an extension of that concept with primorials to determine the seed primes that will be used to produce the unique modular signature of each positive integer.

**Theorem 1.** Every integer, N, > 0, has a unique modular signature under the prime numbers less than or equal to the maximum seed prime for N’s modular signature, \(P_Z\).

Proof.
1. Assume that M and N are two different positive integers under \(P#\), the smallest primorial greater than both, where M ≠ N.
2. Let Q = the set of seed primes of primorial \(P#\), with the largest element of Q equal to \(P_Z\).
3. Let \(X = (r_1, r_2, r_3, \ldots r_Z)\) be the modular signature of M under \(P#\).
4. Let \(Y = (s_1, s_2, s_3, \ldots s_Z)\) be the modular signature of N under \(P#\).
5. Assume \(X = Y\). That is, for every element of \(X\) and corresponding element of \(Y\), \(r_i \equiv s_i \pmod{p_i}\) for each \(p_i \in Q\).
6. By the Chinese Remainder Theorem [8], the set of equations \(U \equiv r_i \equiv s_i \pmod{p_i}\) has a unique solution U modulo \(P#\). Since U is a unique solution, \(U = M\) and \(U = N\), and \(M = N\).
**Theorem 2.** Let N be a positive integer and let A be the smallest primorial greater than or equal to N. If N has a modular signature under the seed primes of A in which all of the modular residues are non-zero, then N will be a prime number.

**Proof.**
1. Let P = the set of seed primes of A that are used to create the modular signature of N.
2. Let $P_N$ be the largest element in P; therefore, $P_N$ is the largest prime $< \sqrt{A}$. Since $N \leq A$, $\sqrt{N} \leq \sqrt{A}$ and $P_N$ is greater than or equal to the largest prime $\leq \sqrt{N}$.
3. Since the modular residue, $s_i$, for every $P_i \in P$ is non-zero in the modular signature of N, N is pairwise co-prime to every element of P.
4. Since N is pairwise co-prime to every seed prime of A, no prime number less than $\sqrt{N}$ is a factor of N. Then N is only divisible by 1 and N, so by definition, N is a prime number.

**Core Versus Non-Core Seed Primes**
Because primorials larger than 30 will have seed primes that are greater than the largest prime factor of the primorial, it will be useful to distinguish between the seed primes which are factors of the primorial and those which are not factors of the primorial.

**Definition:** Let N be a primorial greater than 30, and let $P_N$ equal the largest prime factor of N and $P_{\text{MAX}}$ equal the largest prime $\leq \sqrt{N}$. Then the core seed primes for N will be the primes less than or equal to the largest prime factor of N, $P_N$. The non-core seed primes of N are the remaining seed primes of N, those which are greater than $P_N$ and less than or equal to $P_{\text{MAX}}$.

For example, for primorial 7# = 210 = 2*3*5*7, the core seed primes are the set \{2, 3, 5, 7\} and the non-core seed primes are the set \{11, 13\}. By definition, the two sets are disjoint.

As we saw with primorial 30, the core seed primes of a primorial will generate all possible combinations of their residue values in the modular signatures between 1 and the primorial, inclusive. Further, using the combinatorial Multiplication Principle [9] in a primorial, there will be $X$ combinations of non-zero residues of the N core seed primes, where $X = \prod_{r=1}^{N}(P_r - 1)$ for all primes $P_r \leq P_N$, the largest prime factor of the primorial (the largest core seed prime). All of those combinations will contain residues greater than 0 in their modular signatures for the core seed primes, and all will apply to odd integers.

**Definition:** Let M be a positive odd integer less than a primorial, E. Then M is a potential prime under E if, in its modular signature under E, M has a non-zero modular residue for every core seed prime of E.

Note that the formula for the number of potential primes in a primorial, $X = \prod_{r=1}^{N}(P_r - 1)$ for all primes $P_r \leq P_N$, is equivalent to Euler’s Totient Function [10] when the Totient Function is applied to the primorial.

However, some of the potential primes in the primorial will become composites, because the modular signatures of some of the potential primes will contain residues equal to zero for one or more of the non-core seed primes. For example, as shown in Table 2 below, the modular signature of integer 2291 has all positive residues in its five core seed primes under primorial 2310, but has a zero residue for non-core seed prime 29, because $2291 = 29*79$. Therefore, 2291 was a potential prime number under primorial 2310, but was converted to a composite by a zero residue in its modular signature generated by a non-core seed prime (those greater than $P_r = 11$ and less than or equal to 47).
Further, if none of the potential prime numbers had a zero residue with a non-core seed prime, then the number of prime numbers in primorial 2310 would = 5 + ([2-1]*[3-1]*[5-1]*[7-1] *[11-1]) -1 = 5+480-1 = 484 instead of 343, the actual number of primes less than 2310. The reduction of 141 (29.1%) was due to the impact of the zero residues generated by the 10 non-core seed primes (13 to 47) when they were included in the modular signatures of the potential prime numbers.

Table 2

| Integer | Core Seed Primes | Non-Core Seed Primes |
|---------|------------------|----------------------|
|         | 2  3  5  7 11    | 13 17 19 23 29 31 37 41 43 47 |
| 2,291   | 1  2  1  2  3    | 3  13 11 14 0 28 34 36 32 35 < Signature |

Table 2

Further, if none of the potential prime numbers had a zero residue with a non-core seed prime, then the number of prime numbers in primorial 2310 would = 5 + ([2-1]*[3-1]*[5-1]*[7-1] *[11-1]) -1 = 5+480-1 = 484 instead of 343, the actual number of primes less than 2310. The reduction of 141 (29.1%) was due to the impact of the zero residues generated by the 10 non-core seed primes (13 to 47) when they were included in the modular signatures of the potential prime numbers.

Primorial Stacking
Each primorial > 6 is the product of its predecessor primorial and the next larger prime number in the sequence of primes. Thus, the modular residues under core seed primes 2, 3 and 5 in primorial 5# = 30 = 2*3*5 are repeated 7 times in the modular signatures of primorial 7# = 210 = 30*7 and 77=7*11 times in the modular signatures under primorial 11# = 2310. Similarly, the modular residues under core seed primes 2, 3, 5 and 7 in primorial 210 are repeated 11 times in the modular signatures of primorial 11# = 2310 = 210*11. Of course, each of the modular signatures becomes unique when we include their non-core seed prime residues in each integer’s modular signature under primorial 2310’s seed primes.

Table 3 below illustrates primorial stacking of 5# = 30 = 2*3*5 within primorial 7# = 210 = 30*7. Under primorial 210, the largest prime less than \(\sqrt{210}\) is 13, so the core seed primes of 210 (2, 3, 5 and 7) are joined by two non-core seed primes, 11 and 13.

To illustrate the repetition of the modular signatures of primorial 30 in primorial 210, the odd integers 1 through 195 are grouped in Table 3 in congruence classes Mod 30, each with 7 elements. That is, the class \([1]\) Mod 30 = \{1, 31, 61, 91, 121,151, 181\} for odd integers less than 210. Similar groupings are shown for congruence classes \([3]\), \([5]\), \([7]\), \([9]\), \([11]\), \([13]\) and \([15]\) Mod 30 over the set of odd integers less than or equal to 210, and could be shown for the remaining seven congruence classes for Mod 30 (17, 19, 21, 23, 25, 27 and 29) with similar results covering the remaining odd integers through 209.

In each congruence class, the modular signatures of each member of the class are identical under the core seed primes for 30 = 2*3*5, and differ under seed prime 7. Under primorial stacking, within primorial 210 we would expect to see 7 iterations of the modular signatures of each of the positive integers less than or equal to primorial 30, with the signatures differing in seed primes > 5. For example, within congruence class \([1]\) = \{1, 31,61, …181\} the seven integers have identical modular signatures under core seed primes 2, 3 and 5, and the residues of core seed prime 7 are added to each member of \([1]\) starting with 1 to help create a unique modular signature for each integer under primorial 210.

Further, the residues for non-core seed prime 11 increase by 8 = 30 Mod 11 between corresponding cycles of primorial 30 in each congruence class. That is, the residue for 31 Mod 11 equals 1 Mod 11 + 30 Mod 11 = 1 + 8 = 9. Similarly, the residues for non-core seed prime 13 increase by 4 = 30 Mod 13 between cycles of primorial 30 in each congruence class (e.g. between 1 and 31 Mod 13). Were the modular signatures expanded to include seed primes 17, 19, etc., with the next primorial, then the residues Mod Pr of an integer in each congruence class would increase similarly by s = 30 Mod Pr, with each cycle of 30. In short, there is a pattern to the modular signatures in each congruence class of a primorial.
The same can be said for the other congruence classes Mod 30: the members of each congruence class share identical modular signatures under primorial 30’s core seed primes 2, 3 and 5, and differ under core seed prime 7, with one member in each congruence class receiving the 0 residue from core seed prime 7 in a different cycle of the residues of 7 until 7’s residue cycle starts again after 210.

That pattern will continue when primorial 210 is stacked in the next larger primorial, 11# = 2310 = 210*11. The modular signature of 210 will contain zeros for its core seed primes (2, 3, 5, and 7), causing 211 to restart the cycles of 210’s core seed primes (2, 3, 5, and 7) at residue 1 in each of its multiples within primorial 2310. The core seed primes of 210 (2, 3, 5 and 7) are extended under primorial 2310 with an additional core seed prime (11) and ten non-core seed primes (13, 17, 19, 23, 29, 31, 37, 41, 43, 47). Since the modular signature of 210 is (0,0,0,0) under the core seed primes 2, 3, 5 and 7, when 210 is added to any integer less than 2310, the modular signature of the smaller number will be repeated for the core seed primes of 210. This is illustrated in Table 4 below with two congruence classes of 210 at opposite ends of the primorial: [1] and [209].

Just as the members of the 15 odd congruence classes under Mod 30 had identical modular residues under the core seed primes of 30, when 30 is stacked in 210 and the odd integers are grouped into 105 congruence classes under Mod 210, all of the modular residues of the members of a congruence class are identical under the core seed primes of both 30 and 210, and then differ in the remaining seed primes that make up their modular signatures. As the primorials are stacked further, this property is repeated with the addition of each core seed prime.
This pattern of dispersion of the modular signatures within successive primorials, and the dispersion of the integers with non-zero residues under the core seed primes of a primorial, will be relevant later when we discuss the dispersion of potential primes and potential twin primes within primorials.

### New Composites of Non-Core Seed Primes

Returning to the Sieve of Eratosthenes, we saw that the first new composite (i.e. those not already generated by a smaller prime) for a seed prime \( P_r \) occurred at \( P_r^2 \). We also noted that each new composite thereafter for \( P_r \) is generated as the product of seed prime \( P_r \) and a combination of primes greater than or equal to \( P_r \). Within primorial 2310, for example, the non-core seed prime 13’s first new composite is 169 = 13*13. Its next new composite is 221 = 13*17. 13’s largest new composite in primorial 2310 is 2249 = 13*173. There are larger composites in primorial 2310 that have 13 as a factor (e.g. 2275 = 5*13*17), but those composites were generated first by primes smaller than 13. In fact, when we partition the positive integers into primorials, and examine only the composites generated by the primorial’s non-core seed primes, we can see that all of the prime factors of the “new composite” integers generated by the non-core seed primes in a primorial are contained within the next smaller primorial.

#### Theorem 3: Under modular signatures for a primorial \( E \), the first new composite (i.e. not already generated by a smaller prime) generated by a seed prime of \( E \), \( P_r \), will occur at \( P_r^2 \). All composites less than \( P_r^2 \) in \( E \) will contain a prime factor less than \( P_r \).

**Proof.**

1. Let \( A \) be any composite positive integer less than \( P_r^2 \) in \( E \).
2. By definition, \( A \) has a prime divisor \( X \) with \( 1 < X < A \), thus \( A = XY \).
3. Either \( X \leq \sqrt{A} \) or \( Y \leq A \). Otherwise, if \( X > \sqrt{A} \) and \( Y > \sqrt{A} \), then \( XY > \sqrt{A} \times \sqrt{A} = A \).
4. Therefore, if \( A \) is a composite number less than \( P_r^2 \), it has a prime divisor less than \( P_r \), since \( \sqrt{A} < P_r \).
**Corollary 3.1:** Let $M$ be a primorial and let $E$ be the smallest primorial larger than $M$. If $C_i$ is a new composite of $E$ generated by a non-core seed prime, $P_r$, of $E$, then the other prime factors of $C_i$ will be $< M$.

Proof.
1. Let $P_N$ be the largest prime factor of $E$ such that $E = M \cdot P_N$.
2. Since $P_r$ is a non-core seed prime of $E$, $P_N < P_r$.
3. By Theorem 3, the first composite in $E$ of a non-core seed prime, $P_r$, will be $P_r^2$.
4. Then $P_r^2 < M$.
5. By definition, $C_i$ has a divisor $X$ with $P_r^2 \leq P_r \cdot X < E$.
6. Then $P_r \leq X < (E / P_r)$ and $P_r \leq X < ((M \cdot P_N) / P_r)$.
7. Since $P_N < P_r$, $X < M$, and any prime factor of $X$ will be less than $M$.

**Corollary 3.2:** Let $N$ be a potential prime number under the core seed primes of primorial $E$, with $N$ not equal to any non-core seed prime of $E$. Let $Q$ equal the set of non-core seed primes of $E$. If $N < P_N^2$, where $P_N$ is the smallest element of $Q$, then the modular residue of $N \mod P_S$ will be greater than zero for all $P_S \in Q$.

Proof:
1. By definition of a potential prime, the modular signature of $N$ will not contain a zero residue for any of the core seed primes of $E$.
2. Assume $N$ is a composite of $P_N$, with $N < P_N^2$.
3. By Theorem 3, since $N$ is a composite $< P_N^2$, it must contain a prime factor less than $P_N$. Since $P_N$ is the smallest non-core seed prime of $E$, the prime factor less than $P_N$ must be a core seed prime of $E$.
4. However, since $N$ is a potential prime of $E$, it cannot have a prime factor equal to a core seed prime of $E$.
5. Then $N \neq 0 \mod P_N$ and the modular residue of $N \mod P_N$ is greater than zero.
6. Let $P_S \in Q$ be the first element of $Q$ which is a factor of $N$.
7. Since $N < P_N^2$, and $P_N$ is the smallest element of $Q$, $N = X \cdot P_S$ for some $X < P_N$. However, since $N$ is a potential prime of $E$ and $P_N$ is not a factor of $N$, there cannot exist a prime number $X < P_N$ that is a factor of $N$. Therefore, $N \mod P_S > 0$ for all $P_S \in Q$.

**Formula for Computing the Number of Primes in a Primorial**

Generally, the Sieve of Eratosthenes takes this form for the number of primes less than a positive integer, $N$:

$$\pi (N) = N - 1 + n(SP) - n(\text{Composites of SP})$$

(1)

where 1 is subtracted since 1 is not a prime by definition, $SP$ equals the set of seed primes for $N$, $n(SP)$ is the number of seed primes and $n(\text{Composites of SP})$ is the number of unique elements in the set of composites less than or equal to $N$ that are generated by the seed primes. For example, $\pi (100) = 100 - 1 + 4 - (117 - 45 + 6 - 0) = 25$.

Further, since the seed primes can be divided into two discrete sets of core and non-core seed primes, the composites of the seed primes can be divided into two sets: $A =$ the composites generated by the core seed primes and $B =$ the new composites generated by the non-core seed primes. By the Inclusion-Exclusion Principle [11],

$$n(\text{Composites of SP}) = n(A) + n(B) - n(A \cap B)$$

(2)

Define $P$ as the set of prime numbers and $P_c$ as the set of core seed primes for $N$, and $P_{nc}$ as the set of non-core seed primes for $N$, then create the set of new composites in $A$ by multiplying each element $p_r$ of $P_c$ by...
primes greater than or equal to \( p_r \), such that their product is less than or equal to \( N \). Similarly, create the set of new composites in \( B \) by multiplying each element \( p_r \) of \( P_{nc} \) only by primes greater than or equal to \( p_r \), such that their product is less than or equal to \( N \). Then the number of elements in \( (A \cap B) \), \( n(A \cap B) \), equals 0 since the composites in \( B \) will have no factors from among the core seed primes and therefore will not equal any of the composites in \( A \) (i.e. \( A \cap B \) is the empty set, and \( A \) and \( B \) are disjoint sets).

Now define an alternate form of the sieve of Eratosthenes for primorials. For primorial \( E \),

\[
\pi(E) = n(CSP) + \left( \prod_{r=1}^{M}(P_r - 1) \right) - 1 - n(B)
\]

where \( P_r \) are the \( M \) core seed primes of \( E \), CSP is the set of core seed primes of \( E \) (non-core seed primes are counted within \( \prod (P_r - 1) \)), and \( B \) is the set of new composites generated by the non-core seed primes of \( E \). The product of the core seed primes of \( E \), \( \prod (P_r - 1) \), will generate all possible combinations of the non-zero residues of the core seed primes in the modular signatures of the integers from 1 to \( E \). Those are all potential prime numbers, including 1 (which is subtracted in the formula). However, some of those potential primes will become composites when the non-core seed primes add one or more \([0]\) residue elements to their modular signatures. That was illustrated for 2291 in Table 2, because of the zero-residue added by 29 in 2291 = 29 x 79.

Therefore, we need to determine if there is a pattern to when the non-core seed primes eliminate potential prime numbers from the set of potential prime numbers that could be twin primes, knowing that each non-core seed prime generates new composites using prime factors greater than or equal to itself and less than the next smaller primorial. Establishing that pattern enables the proof.

**Modular Residue Cycles**

Consider the behavior of the residues of the integers under modular arithmetic, extending the picture illustrated in Table 1 to include an additional prime, 7. As we move down the column of integers, incrementing each by adding 1 to the preceding value, we move through the modular remainders in a synchronized way.

Note that each seed prime operates a repeating cycle consisting of its residues through successive positive integers, all starting where \( A = 1 \). As we increment \( A \) by 1 (i.e. cycle through the integers), each mod residue increases by 1. And each seed prime, \( P_r \), in turn, will complete a full cycle (equal in length to twice the prime for the odd integers) at a different point, because each possesses \( P_r \) residues, with the difference in the ending integer between two primes determined by the size of the gap between the two primes.

It should now be obvious that there is a logic to when the prime numbers appear within the set of positive integers. A prime appears within a primorial when each residue of its modular signature under each smaller seed prime is non-zero, and its own modular residue equals 0 for the first time. That happens in the modular signature of a prime number when the repeating sequence of modular residues of the seed primes all fall on a non-zero value for each seed prime except for the prime itself. As noted earlier, the powers of a prime number (e.g. \( 7^2 = 49 \)) can also have a single 0 residue in their modular signature, but they will not be a prime because they will not be the first occurrence of that 0 residue among the integers for that seed prime (e.g. 7 is the first occurrence of the 0-residue mod 7, while 49 is not, so 49 is divisible by both 7 and 49).

**Potential Prime and Non-Core Seed Prime Composite Patterns**

In finding the number of primes in a primorial, the two main variable components are (1) the number of potential prime numbers generated by all possible combinations of the non-zero residues of the core seed
primes (thereby eliminating the composites of the core seed primes), and (2) the number of new composites generated with a zero residue by each of the non-core seed primes in the modular signatures of each odd number, thereby converting some of the potential primes into composites. Table 5 below illustrates how the number of core seed prime residues and non-core seed prime residues are distributed within a primorial (in this case, primorial $2,310 = 2*3*5*7*11$) over the odd integers, $1 – 2,309$.

| Primorial: | 2310 | Square root: | 48.06 | Max Seed Prime: | 47 |
|-----------------|--------|--------------|--------|----------------|----|
| Cycle Length: | 2 6 10 14 22 26 34 38 46 58 62 74 82 86 94 |
| # Cycles: | 1155 385 231 165 105 | 88.85 67.94 60.79 50.22 | 39.63 37.26 31.22 28.17 26.86 24.57 |

Table 5

The table shows the number of times a residue is used by each seed prime in the 1155 modular signatures of the odd integers in the primorial. For a core seed prime, the core seed prime’s residues are used the same number of times (e.g. for core seed prime 5, each of its residues is used 231 times in the odd integers) within primorial 2310. In contrast, the last cycle of each non-core seed prime is not...
completed, so the number of some of the even residues (which always come later in the cycle for odd numbers) will be one less than the number of odd residues for each non-core seed prime.

The length of a seed prime’s cycle for odd integers in Table 5 is two times the seed prime, since the cycle is skipping the even numbers. Thus, \# Cycles = Primorial / Cycle Length, with the number of cycles inversely proportional to the size of the seed prime. And as Table 5 shows, the core seed primes have complete cycles because they are all prime factors of primorial 2310, while the last cycle of each non-core seed prime is incomplete. Further, the table illustrates that as the non-core seed primes increase in size, they have a diminished impact on the potential primes in the primorial since they only have one zero residue per cycle and each prime’s cycle is longer as each prime gets larger.

Using the cycle of the largest non-core seed prime (47) in primorial 2310, Table 6 below shows the interplay of the number of potential primes by cycle for the largest non-core seed prime (47), and the number of new composites generated by each of the non-core seed primes for the matching odd numbers in each cycle. The new composites manifest themselves as a 0 residue in the modular signature of each odd integer from 1 - 2309 for the applicable non-core seed prime.

Table 6

![Table 6](image)

The table assigns the new composite to the non-core seed prime which is the smallest factor of the composite (or first 0 residue among the non-core seed prime portion of the modular signature of the potential prime). Then, 480 potential primes are reduced by the 141 new composites to produce 339
“survivor” potential primes. Those are added to the 5 core seed primes, reduced by 1 for the number 1, to yield the total number of primes for 2310: 343.

The number of potential primes is fairly consistent from one cycle to the next, varying primarily because of the different gap sizes between primes causing an overlap with the cycle cutoff. Therefore, to produce the gradually smaller number of primes per cycle, we expect the cumulative number of new non-core seed prime composites to increase gradually as the cycles unfold, starting with \( P_r^2 \) for each non-core seed prime \( P_r \). Further, because each of the non-core seed primes starts its new composites at \( P_r^2 \) and new composites appear thereafter when multiplied by a prime greater than or equal to the non-core seed prime \( P_r \), we expect the number of new composites within a primorial to decline as the value of the non-core seed prime (and cycle length) increases. That is exactly what happens as shown in Table 6, as the new composites decline from 36 to 1 over the non-core seed primes (13 to 47).

Figure 1 below depicts graphically the number of new non-core seed prime composites for the next larger primorial, 30,030 = 2310 * 13. The non-core seed primes (17 through 173) generated 2,517 new composites (i.e. composites in which the non-core seed prime was the smallest prime factor).

The formula for the line of best fit, \( Y = 426.65e^{-0.027x} \), is not a perfect fit to the actual data, but in the aggregate produces 2516.9 composites from the non-core seed primes versus an actual count of 2517. Therefore, in our equation for the number of primes in a primorial,

\[
\pi (E) = n(CSP) + ( \prod (P_r - 1) ) -1 - n(B)
\]

we can determine \( n(B) \), the number of non-core seed prime composites, with 100% accuracy using the combinatorial principle of Inclusion and Exclusion [12] for the 34 non-core seed primes or to a high degree of accuracy using a decay function on base-e. However, per Theorem 3, for our purposes it is only necessary to know that the number of new composites generated by each non-core seed prime, \( P_r \), begin at \( P_r^2 \).
Figure 2 below depicts graphically a different view of the same non-core seed prime composite data for primorial 30,030 along with the potential primes, by cycle of the largest seed prime (and largest non-core seed prime), 173. The core seed primes (2, 3, 5, 7, 11 and 13) generated a total of 5,760 potential primes among the odd integers, and the non-core seed primes (17 through 173) generated 2,517 unique new composites. Thus, the number of primes for primorial 30,030 = \(\pi(30,030) = 6 + 5,760 - 1 - 2,517 = 3,248\), where 6 is the number of core seed primes for primorial 30,030 and 1 is subtracted from 5,760 because it is included in the potential primes but is not a prime number by definition.

As expected because of the cycling of the modular residues in the modular signatures of the core seed primes, the number of potential primes is fairly constant across each cycle of the largest non-core seed prime (cycle length = 2 * 173 = 346), varying primarily because of the different gap sizes between primes causing an overlap with the cycle cutoff. Therefore, to produce the gradually smaller number of primes per cycle characteristic of prime numbers, we expect the cumulative number of new non-core seed prime composites to increase gradually as the cycles unfold, starting at \(P_r^2\) for each non-core seed prime \(P_r\). That is exactly what happens as shown in Figure 2.

![Figure 2](image-url)  

The consistent distribution of the potential primes across the span of the primorial is understandable in light of two factors: (1) primorial stacking and (2) the multiplicative property of the Euler Totient Function, \(\phi(n)\). [13]

**Theorem 4**: Let \(A\) equal a primorial whose largest prime factor (and therefore, its largest core seed prime) is \(P_M\), and let \(B\) equal the next larger primorial with largest prime factor \(P_N\). Then the number of potential primes in \(B = \phi(B) = \phi(A)\phi(P_N)\), where \(\phi(P_N) = P_N - 1\). On average, \(\phi(B) / P_N\) potential primes of \(A\) will be repeated in each cycle of \(A\) within \(B\).

Proof.
1. Since B is the next larger primorial after A, B = A*P_N and the number of potential primes in B = \(\varphi(B) = \varphi(A)\varphi(P_N)\) by the multiplicative property of the Euler Totient function.

2. Since P_N is a prime number, \(\varphi(P_N) = P_N - 1\).

3. Each potential prime in A contains a modular signature on the core prime factors in A, and each potential prime's modular signature in A is repeated P_N times in the modular signatures of B. However, when the core seed primes of A are supplemented by the core seed prime P_N of B, one of the modular signatures of a potential prime in A will contain a 0 residue from the congruence classes of P_N, leaving just P_N - 1 non-zero residues for the potential primes of A in each cycle of B. Thus, on average, each cycle of A in B will have \(\lceil(P_N - 1) / P_N\rceil\) potential primes in B.

4. Then on average there will be \(\varphi(A) \times \lceil(P_N - 1) / P_N\rceil = \varphi(B) / P_N\) potential primes of A repeated in each cycle of A within B.

Part 2: Application of Modular Signatures to the Twin Primes Conjecture

If the number of potential primes is fairly consistent across the cycle of the largest seed prime, can we expect the number of potential twin primes to be fairly consistent within primorial cycles? And can we expect the number of twin prime pairs to decline as the cycle count increases because of the increasing number of composites that will "knock out" potential twins from being true twins? And can we determine when the first potential twin prime will be converted to a “false” twin (or a composite) by a non-core seed prime’s zero residue in the modular signature of the potential twin prime?

Table 7 below shows how the core seed primes generate potential twin primes among the potential primes for primorial 13# = 30030 = 2*3*5*7*11*13 = 2310*13. On average, the core seed primes generate 443 potential primes in each cycle of primorial 2310 in the primorial 30030. And on average, the seed primes generate 114 potential twins among those potential primes in each cycle of 2310 within 30030.

| Cycle - Primorial 2310 | Cumulative Number | Number In Cycle |
|------------------------|-------------------|-----------------|
| Count | Potential Primes | Potential Twins | FALSE Twins | TRUE Twins | Potential Primes | Potential Twins | FALSE Twins | TRUE Twins |
| 1 | 2310 | 443 | 114 | 47 | 67 | 443 | 114 | 47 | 67 |
| 2 | 4620 | 887 | 229 | 112 | 117 | 444 | 115 | 65 | 50 |
| 3 | 6930 | 1329 | 344 | 186 | 158 | 442 | 115 | 74 | 41 |
| 4 | 9240 | 1772 | 456 | 266 | 190 | 443 | 112 | 80 | 32 |
| 5 | 11550 | 2215 | 571 | 345 | 226 | 443 | 115 | 79 | 36 |
| 6 | 13860 | 2658 | 685 | 430 | 255 | 443 | 114 | 85 | 29 |
| 7 | 16170 | 3102 | 800 | 515 | 285 | 444 | 115 | 85 | 30 |
| 8 | 18480 | 3545 | 914 | 593 | 321 | 443 | 114 | 78 | 36 |
| 9 | 20790 | 3988 | 1029 | 677 | 352 | 443 | 115 | 84 | 31 |
| 10 | 23100 | 4431 | 1142 | 753 | 389 | 443 | 113 | 76 | 37 |
| 11 | 25410 | 4873 | 1256 | 846 | 410 | 442 | 114 | 93 | 21 |
| 12 | 27720 | 5317 | 1371 | 932 | 439 | 444 | 115 | 86 | 29 |
| 13 | 30030 | 5760 | 1485 | 1019 | 466 | 443 | 114 | 87 | 27 |

Note: "True Twins" in the first cycle excludes 5, 7, and 13; their predecessor had 0 in the modular residue

Table 7

That result is expected given our earlier discussion of the multiplicative nature of the Euler Totient Function, and as discussed below, the multiplicative nature of the function used to determine the number of potential twin primes. The reason: the repeating cycle of the modular residues of the seed primes in the modular signatures of each odd integer creates a consistent distribution of the non-zero residues in each cycle of smaller primorials within a larger primorial due to primorial stacking.
Further, consistent with Theorem 3, we would have expected the first new composite of primorial 13# = 30030 to convert a potential twin prime to a composite to appear when the first non-core seed prime, 17, equals $17^2 = 289$. However, 289 is not a potential twin prime because the odd numbers on either side of it (287 and 291) are not potential primes. Similarly, 323 = $17*19$ is also not a potential twin prime for the same reason as 289. Consequently, the first new composite of a non-core seed prime to convert a potential twin prime to a composite in primorial 30030 is 361 = $19^2$. Therefore, because the set of potential twin primes is a subset of the set of potential primes, we can expect the first new composite of a non-core seed prime, $P_r$, to convert a potential twin prime to a composite no earlier than $P_r^2$, and it may happen later.

**Predicting Potential Twin Primes From Modular Signatures**

It is notable that there is a pattern in the modular residues that predicts when a potential prime can be a potential twin prime for two consecutive odd integers, $O_1$ and $O_2$ (with $O_1 < O_2$), where $s_i$ is the modular residue for a core seed prime, $P_r$:

- If $s_i = 0$ in the modular signature of $O_1$ for a core seed prime, then $O_1$ will not be a potential prime.
- If $s_i = P_r - 2$ in the modular signature of $O_1$ for a core seed prime $P_r$, then $O_2 = O_1 + 2$ will not be a potential prime (and therefore, not a potential twin) since the second odd integer in the pair will be a composite.

The pattern is illustrated in Table 8 below which shows the modular signatures for ten consecutive odd integers within primorial 11# = 2310, where the largest core seed prime is 11 and the largest non-core seed prime (the largest prime less than $\sqrt{2310}$) is 47. Four of the odd integers are prime numbers, five are potential primes and just two are potential twin primes.

| Primes | Odds | Delta vs Potential Twin Prime | Core Seed Primes | Non-Core Seed Primes | Potential Prime |
|--------|------|-------------------------------|------------------|----------------------|-----------------|
|        |      |                               |                  |                      |                 |
| x      | 2237 | 2                             |                  |                      |                 |
| x      | 2239 | 2                             |                  |                      |                 |
|       | 2241 | 2                             |                  |                      |                 |
| x      | 2243 | 2                             |                  |                      |                 |
|       | 2245 | 2                             |                  |                      |                 |
|       | 2247 | 2                             |                  |                      |                 |
|       | 2249 | 2                             |                  |                      |                 |
| x      | 2251 | 2                             |                  |                      |                 |
|       | 2253 | 2                             |                  |                      |                 |
|       | 2255 | 2                             |                  |                      |                 |

**Table 8**

2237 and 2239 are both prime numbers because there are no residues equal to zero for either the core seed primes or the non-core seed primes in their modular signatures, and 2239 is a potential twin because both 2237 and 2239 are potential primes. 2241 is not a potential prime because it has a zero modular residue under Mod 3, not surprising because its predecessor, 2239, had 1 for the modular residue under Mod 3, and $1+2 = 0 \mod 3$. For the same reason, 2247 and 2253 are not potential primes. Similarly, 2245 is not a potential prime because 2243 had 3 for the modular residue under Mod 5, and $3+2 = 0 \mod 5$. For the same reason, 2255 is not a potential twin. The same type of residue combinations under Mod 7 caused 2245 to not be a potential prime, or a potential twin prime.

Therefore, let $P$ equal the set of seed primes for a primorial $M$, and let $n(P) = m$. Then a formula for computing the number of potential twin primes in primorial $M$ (with $P_m$ equal to the largest core seed prime) is to calculate the product of the primorial’s core seed primes, excluding two residues (0 and $P_r - 2$)}
from each core seed prime, $P_r$, in the calculation of the potential twin primes, and starting from 3 (the second prime factor, since the residue for odd numbers under Mod 2 is always equal to 1):

$$T(M) = \left(3 - 2\right)\left(5 - 2\right)\left(7 - 2\right)\ldots\left(P_m - 2\right) = \prod_{P_{r=3}}^{P_m} (P_r - 2)$$  \hspace{1cm} (5)

The result of the formula for the number of potential twin primes, $T(M)$, excludes the first three actual twin primes (5, 7 and 13) since they are not potential primes (they each have a zero residue in their modular signature) and includes the number 1. Like the formula for potential primes in a primorial, the formula for the number of potential twin primes is multiplicative because it is based on primorial stacking. That is, if $M$ is a primorial whose prime factors are the set $P = \{2, 3, 5, \ldots, P_m\}$ and $N$ is the next larger primorial whose largest prime factor is $P_N$, then it follows that

$$T(N) = T(M) \times (P_N - 2)$$  \hspace{1cm} (6)

and we will have a relatively consistent distribution of the potential twin primes within the primorial $N$.

**Potential Twin Primes Under Primorial Stacking**

Next, consider how the number of potential twin primes in each primorial changes under primorial stacking. That is, when we consider two or more primorials, will the average number of potential twin primes in the smaller primorial remain constant in each cycle within the larger primorial, or be smaller because of the additional core seed primes in the larger primorial?

Table 9 below illustrates the increasing number of potential twin primes in each primorial as the primorials grow. The number of potential primes is calculated using Euler’s Totient Formula. The number of potential twin primes is calculated using Equation (5) above for the number of potential twin primes in a primorial $M$, with each potential twin factor in column 6 being 2 less than the corresponding prime factor for the primorials in column 2.

| Count | Prime | Number Of Cycles By Prior Prime | Potential Prime Factors | Number Potential Primes In Primorial | Number Potential Twins In Each Prior Primorial | Avg Number Potential Twins In Each Prior Primorial Cycle |
|-------|-------|---------------------------------|--------------------------|---------------------------------------|-----------------------------------------------|----------------------------------------------------------|
| 1     | 2     | 1                              |                          |                                       |                                               |                                                          |
| 2     | 3     | 6                              | 2                        | 1                                    |                                               |                                                          |
| 3     | 5     | 30                             | 4                        | 3                                    | 8                                            | 3                                                        |
| 4     | 7     | 210                            | 7                        | 6                                    | 5                                            | 48                                                       | 15                                                       | 2.1                                                      |
| 5     | 11    | 2,310                          | 11                       | 10                                   | 9                                            | 480                                                      | 135                                                      | 12.3                                                     |
| 6     | 13    | 30,030                         | 13                       | 12                                   | 11                                           | 5,760                                                    | 1,485                                                    | 114.2                                                    |
| 7     | 17    | 510,510                        | 17                       | 16                                   | 15                                           | 92,160                                                   | 22,275                                                   | 1,310.3                                                  |
| 8     | 19    | 9,699,690                      | 19                       | 18                                   | 17                                           | 1,658,880                                                | 378,675                                                  | 19,930.3                                                 |
| 9     | 23    | 223,092,870                    | 23                       | 22                                   | 21                                           | 36,495,360                                               | 7,952,175                                                | 345,746.7                                                |
| 10    | 29    | 6,469,693,230                  | 29                       | 28                                   | 27                                           | 1,021,870,080                                            | 214,708,725                                              | 7,403,749.1                                              |
For example, the number of potential twins in primorial 2310 is 135. Primorial 2310 then has 13 cycles in primorial 30030. If each of those cycles contained 135 potential twin primes, then there would be 1755 potential twin primes in primorial 30030. However, there are only 1485 potential twins in primorial 30030. The reduction is expected, since the potential twin primes under primorial 30030 are subjected to an additional factor (13-2) in Equation (5) to produce the number of potential twin primes in 30030. Therefore, the average number of potential twin primes in M = 2310 is reduced to 135*(11/13) = 114 in each cycle of the 13 cycles of M within N = 30030 so that the total number of potential twin primes in N will remain T(M) * (13-2) = 1485.

While the average number of potential twin primes in a primorial is reduced within larger primorials, note that there are potential twins in every cycle, with only a small variance between each, as shown in Table 7. That is due to the repeated cycling of the modular residues of each core seed prime within each stacked primorial, so that the modular signatures of the integers in a primorial are repeated in each larger primorial (primorial stacking).

**Theorem 5**: Let M equal a primorial > 30 and let N equal a primorial greater than M. Let $P_M$ equal the largest prime factor of M, let $P_S$ be the smallest prime number greater than $P_M$ and let $P_Z$ equal the largest prime factor of N (i.e., $N = M*P_S...P_Z$). Let $T(M)$ equal the number of potential twin primes in M under the core seed primes of M, and let $T(M)$ equal the average number of potential twin primes in each cycle of M under the core seed primes of N. Then, the number of potential twin primes of N equals $T(N) = T(M) \times \prod_{Pr=P_Z}^{Pr=P_S} (Pr - 2)$, where Pr equals a prime number, and on average there will be $T(M) = T(N) / \prod_{Pr=P_S}^{Pr=P_Z} (Pr - 2)$ potential twin primes in each cycle of M in N.

Proof.
1. $N = 2*3*5...P_m*P_S...P_Z$.
2. By Equation (5), $T(N) = \prod_{Pr=P_S}^{Pr=P} (Pr - 2)$
3. By Equation (5), $T(M) = \prod_{Pr=P_M}^{Pr=P} (Pr - 2)$.
4. $T(N) = \prod_{Pr=P_M}^{Pr=P} (Pr - 2)$.
5. $T(N) = T(M) * \prod_{Pr=P_S}^{Pr=P} (Pr - 2)$ over the core seed primes of N.
6. Since there are $\prod_{Pr=P_S}^{Pr=P} (Pr - 2)$ cycles of M in N, on average there will be $T(M) = T(N) / \prod_{Pr=P_S}^{Pr=P} (Pr - 2)$ potential twin primes in each cycle of M in N.
7. $T(M) = T(N) / \prod_{Pr=P_S}^{Pr=P} (Pr - 2)$
8. $T(M) = T(M) * \prod_{Pr=P_S}^{Pr=P} (Pr - 2) / \prod_{Pr=P_S}^{Pr=P} (Pr)$
9. $T(M) = T(M) * \prod_{Pr=P_S}^{Pr=P} (Pr - 2) / \prod_{Pr=P_S}^{Pr=P} (Pr)$ potential twin primes in each cycle of M in N on average.

Table 10 below shows groups of three primorials with a specific relationship. A is the smallest, B is the next largest, and C is the primorial whose largest factor is the largest prime < $\sqrt{B}$. The largest core seed prime of A is labeled Pn-a; the largest of B is Pn-b, and the largest of C is Pn-c. Observe the following in the table:

- Starting with the second iteration of primorials A-B-C, each new primorial A equals the prior primorial B. Consequently, the largest core seed primes also reflect that rotation.
- The number of potential twin primes in A, $T(A)$, is calculated using Equation (5) and is shown in column 8. Those values are multiplied by a product factor in column 9 to get the average number of potential twin primes in each cycle of A within C, Avg $T(A)$ in C in column 10. The product factor is equal to $\prod_{Pr=P_S}^{Pr=P} (Pr - 2)/Pr$, where Pn-b is the largest core seed prime (factor) of B and Pn-c is the largest core seed prime (factor) of C. That is, the product factor is calculated using the prime factors that are greater than those in A and less than or equal to those in C. Alternatively, the
average value of $T(A)$ in $C$ can be derived by using Theorem 4: calculate $T(C)$ and divide $T(C)$ by the product of the core seed primes between $P_{n-b}$ and $P_{n-c}$ inclusive.

- Note that while the primorials $A$, $B$ and $C$ grow very rapidly, the largest core seed primes grow much more slowly. The consequence is that the product factor, which is less than 1 and is derived from the core seed primes, does not shrink as quickly as the primorials grow, so that the average $T(A)$ in $C$ continues to grow rapidly.

- The last two columns of the table show the best fit curve for the relationship between the product factor in column 9 and the largest core seed prime of primorial $C$ in column 7. The first four equations were calculated directly from the individual data points, while the last four equations were interpolated to produce the calculated value of $T(A)$ in $C$.

| Primorials | Largest Core Seed Prime | Potential Twin Primes of A | Best Fit Power Curve* |
|------------|-------------------------|---------------------------|-----------------------|
| $A$ | $B$ | $C$ | $P_{n-b}$ | $P_{n-c}$ | $T(A)$ in $A$ | Product Factor | $\text{Avg } T(A)$ in $C$ | $M$ | $N$ |
| 1 | 210 | 2,310 | 47# | 7 | 11 | 47 | 15 | 0.37532 | 5 | 2.46030 | -0.50000 |
| 2 | 2,310 | 30,030 | 173# | 11 | 13 | 173 | 135 | 0.26007 | 35 | 2.41090 | -0.43700 |
| 3 | 30,030 | 510,510 | 709# | 13 | 17 | 709 | 1,485 | 0.19284 | 286 | 2.13640 | -0.37100 |
| 4 | 510,510 | 9,699,690 | 3,109# | 17 | 19 | 3,109 | 22,275 | 0.14687 | 3,272 | 1.78580 | -0.31500 |
| 5 | 9,699,690 | 223,092,870 | 14,929# | 19 | 23 | 14,929 | 378,675 | 0.11252 | 43,632 | 1.37507 | -0.25830 * |
| 6 | 223,092,870 | 6,469,693,230 | 80,429# | 23 | 29 | 80,429 | 7,952,175 | 0.09147 | 727,428 | 0.97217 | -0.20922 * |
| 7 | 6,469,693,230 | 200,560,490,130 | 447,829# | 29 | 31 | 447,829 | 214,708,725 | 0.07405 | 15,900,087 | 0.67181 | -0.16947 * |
| 8 | 200,560,490,130 | 7,420,738,134,810 | 2,724,079# | 31 | 37 | 2,724,079 | 6,226,553,025 | 0.06105 | 380,157,930 | 0.46677 | -0.13727 * |

Table 10

Figure 3 illustrates the typical shape of the function relating the product factor to $P_{n-c}$, the largest core seed prime of primorial $C$. In this example, $A = 17\# = 510,510$ and $B = 19\# = 9,699,690$, so the product factors start with $P_{n-b} = 19$ and grow to $P_{n-c} = 3109$. The average $T(A)$ in $C = T(A) \times \text{Product Factor} = 22,275 \times 0.14687644 = 3,272$.

As $P_{n-c}$ increases from 19 to 3109 (the largest core seed prime in $C$), the impact of each successive factor, $(Pr-2)/Pr$ on the product factor, diminishes as the primes grow and the individual factors approach 1. Consequently, as primorials $A$, $B$ and $C$ increase, the diminished impact of the product factor, combined with the growing average gap between primes, ensures that the average number of potential twin primes of $A$ in $C$, $T(A_C)$, is greater than 1 and each successive $T(A_C)$ is larger than its predecessor.
Theorem 6: Let A > 30 be a primorial and let B be the smallest primorial larger than A. Let Pb = the largest core seed prime of B, such that B = A * Pb. Let Pc be the largest prime < √B and let primorial C = Pc#. Let T(A#) equal the number of potential twin primes of A in A and T(Ac) equal the average number of potential twin primes in each cycle of A in C, and T(B#) equal the average number of potential twin primes in each cycle of B in C. Then T(B#) > T(A#) ≥ 5 and (T(B#) – T(A#)) > 5.

Proof.
1. Let PNA = the largest core seed prime of A.
2. By Equation (5), T(A#) = (3-2)(5-2)…(PNA -2)
3. By Equation (5), T(B#) = (3-2)(5-2)…(PNA -2)(Pb – 2) = T(A#) * (Pb – 2)
4. By Theorem 5, T(Ac) = T(A#) * ⋂Pr ((Pr – 2)/Pr), where Pr = a prime number
5. By Theorem 5, T(Bc) = T(C) / ⋂Ps (Pr), where Ps is the next larger prime than Pb
6. By Theorem 5, T(Ac) = T(C) / ⋂Ps (Pr)
7. Since Pb*⋂Ps (Pr) = ⋂Ps (Pr), T(Bc) = T(Ac) * Pb
8. Since T(Ac) = 5 for the combination of primorials (A = 210, B = 2310 and C = 30030), where 210 is the smallest primorial > 30, then T(Ac) ≥ 5 for A ≥ 210
9. Since T(Bc) = Pb * T(Ac), Then T(Bc) – T(Ac) > 5 for A ≥ 210

Theorem 7: Let A equal a primorial whose largest prime factor (and therefore, its largest core seed prime) is PN. If Pz equals the smallest non-core seed prime of A, the potential primes and the potential twin primes that are less than (Pz)² in A will not be converted to composites; they will remain prime numbers.

Proof.
1. Let Q = the set of seed primes for A, with P is a member of Q.
2. Under the combinatorial multiplication principle, the core seed primes of A (2, 3, 5,…PN) will generate all possible combinations of modular residues for the integers from 1 to A under its core seed primes. The number of potential prime numbers in A will equal φ(A) and by Equation (5) the number of potential twin primes in A will equal T(A) = ⋂Pr=3 (Pr-2) for primes Pr = 3 to PN.
3. There will be no zero residues in the modular signatures of all potential primes and potential twin primes under the core seed primes in A, by virtue of the formulas used to generate them.
4. By Theorem 3, since Pz equals the smallest non-core seed prime of A, (Pz)² will be the first new composite generated by the non-core seed primes of A.
5. Since (Pz)² will be the first new composite generated by the non-core seed primes of A, by Corollary 3.2 the modular signatures of all potential primes (and potential twin primes which are also potential primes) that are less than (Pz)² will not have any zero modular residues under the non-core seed primes of A; instead, the modular signatures of all potential primes and potential twin primes that are less than (Pz)² will only contain non-zero residues under the non-core seed primes of A.
6. Since any potential primes and potential twin primes < (Pz)² in A will have no zero residues in their modular signatures, by Theorem 2 they will remain prime numbers.
Part 3: Proof of the Twin Primes Conjecture

To prove the twin primes conjecture, we will need to do the following: (1) Assume there is a largest prime number, N, that is the last twin prime and (2) create a scaffold of three primorials greater than N, such that the middle primorial is large enough to contain potential twin primes greater than N and the square of the smallest non-core seed prime of the largest primorial is greater than the second primorial. See Appendix 1 for a model of the elements of this proof.

Proof.

1. Assume N > 31 since there are twin primes ≤ 31.
2. Let \( T_W \) = the set of all twin primes and assume that \( T_W \) is a finite set. Let \( K_N \) = the number of elements in \( T_W \). Then \( K_N \) is the maximum number of twin primes among all positive integers.
3. Assume N is the largest odd prime which has a twin prime equal to N-2. That is, any other prime greater than N does not have a twin prime.
4. Let \( A \) = the smallest primorial > N, and let \( P_{\text{MAX-A}} \) = the largest prime factor of \( A \). That is,
   \[
   A = 2*3*5*...P_{\text{MAX-A}}.
   \]
5. Let \( B \) = the smallest primorial > \( A \), and let \( P_{\text{MAX-B}} \) = the largest prime factor (and core seed prime) of \( B \). \( P_{\text{MAX-B}} \) is also the smallest prime > \( P_{\text{MAX-A}} \). That is,
   \[
   B = 2*3*5*...P_{\text{MAX-A}*P_{\text{MAX-B}}}.
   \]
6. Let \( P_{\text{MAX-B+1}} \) = the smallest prime > \( P_{\text{MAX-B}} \). \( P_{\text{MAX-B+1}} \) will be the smallest non-core seed prime of \( B \).
7. Let \( P_{\text{MAX-C}} \) equal the largest prime number < \( \sqrt{B} \). \( P_{\text{MAX-C}} \) will be the largest non-core seed prime of \( B \).
8. Let \( C \) = the primorial whose largest factor is \( P_{\text{MAX-C}} \). That is,
   \[
   C = 2*3*5*...P_{\text{MAX-A}*P_{\text{MAX-B}}P_{\text{MAX-B+1}}...P_{\text{MAX-C}}}
   \]
9. Using Equation (5), let \( T(C) \) = the number of potential twin primes of \( C \) under the core seed primes of \( C \).
   \[
   T(C) = (3-2)(5-2)(7-2)...P_{\text{MAX-C}} - 2
   \]
10. Let \( P_{\text{MAX-NC}} \) = the smallest non-core seed prime of \( C \).
11. Let \( Q \) = the set of prime factors of \( C \) that are greater than \( P_{\text{MAX-A}} \), and let \( Z = n(Q) \).
12. Using Equation (5), let \( T(A_A) \) = the number of potential twin primes of \( A \) under the core seed primes of \( A \).
   \[
   T(A_A) = (3-2)(5-2)(7-2)...P_{\text{MAX-A}} - 2
   \]
12. By Theorem 5, \( T(A_C) \) = the number of potential twin primes of \( A \) under the core seed primes of \( C \),
   \[
   T(A_C) = T(A_A) * \prod_{r=1}^{Z} ((Pr - 2)/Pr) \text{ where } Pr \in Q
   \]
   \[
   T(A_C) = T(C) / \prod_{r=1}^{Z} (Pr)
   \]
13. Using Equation (5), let \( T(B_B) \) = the number of potential twin primes of \( B \) in \( B \)
   \[
   T(B_B) = (3-2)(5-2)(7-2)...(P_{\text{MAX-A}} - 2)( P_{\text{MAX-B}} - 2)
   \]
14. By Theorem 5, \( T(B_C) \) = the number of potential twin primes of \( B \) under the core seed primes of \( C \),
   \[
   T(B_C) = T(B_B) * \prod_{r=2}^{Z} ((Pr - 2)/Pr) \text{ where } Pr \in Q
   \]
\[ T(B_C) = \frac{T(C)}{\prod_{r=2}^{Z}(Pr)} \]

15. Then \( T(B_C) - T(A_C) \) is the number of potential twin primes between \( B \) and \( A \) in primorial \( C \).
16. By Theorem 6, \( T(B_C) - T(A_C) > 5 \)
17. Since \( T(B_C) - T(A_C) > 5 \), there are potential twin primes in \( B \) which are greater than \( N \).

Because of the assumption that \( K_N \) is the maximum number of twin primes among all positive integers, all potential twin primes of \( B \) that are greater than \( N \) must be converted to composites by zero residues of the non-core seed primes of \( C \).

18. Since \( P_{\text{MAX-NC}}>\sqrt{B} \), \((P_{\text{MAX-NC}})^2 > B \).
19. Since \((P_{\text{MAX-NC}})^2 > B \), by Theorem 7 no potential twin prime of \( B \) will be converted to a composite, including every potential twin prime in \( B > A > N \) generated by the equation for \( T(B) \).
20. Since every potential twin prime of \( B \) will remain a prime, and there are potential twin primes in \( B > A > N \), there exist twin primes that are greater than any element in \( T_W \). Since \( N \) can be any odd prime number, the assumption is false that \( T_W \) is a finite set. Therefore, there are an infinite number of twin primes.
## Appendix 1

### Model of Twin Primes Proof Elements

| Primorials | Integers | Span of Potential Twin Primes of C | Twin Prime Counts |
|------------|----------|------------------------------------|-------------------|
| C = 2*3*5...PMAX-C | Primorial whose largest core seed prime = PMAX-C | Potential Twin Primes of C | |
| [PMAX-NC]^2 | Since PMAX-NC > VB, [PMAX-NC]^2 > B | | |
| B = 2*3*5...PMAX-B | Smallest primorial > A | Potential Twin Primes of C in B | TC | Number of potential twin primes of C in C |
| PMAX-NC | Smallest non-core seed prime of C | | |
| PMAX-C | Largest prime < \(\sqrt{B}\); largest core seed prime of C | Potential Twin Primes of C in A | TB | Number of potential twin primes of C in B |
| A = 2*3*5...PMAX-A | Smallest primorial > N | | |
| PMAX-B | Largest core seed prime of B; smallest non-core seed prime of A | | TA | Number of potential twin primes of C in A |
| PMAX-A | Largest core seed prime of A | | |
| N | The last twin prime | | Kn | Number of twin primes ≤ N |

Note: Objects Are Not Drawn To Scale
Notes

1. Shanks, Daniel (1962). *Solved and Unsolved Problems in Number Theory*. New York: Spartan Books, p. 30.
2. Neale, Vicky (2017). *Closing the Gap*. Oxford, United Kingdom, Oxford University Press, p. 141-144.
3. Wells, David (2005). *Prime Numbers: The Most Mysterious Figures in Math*. Hoboken, NJ: John Wiley & Sons, Inc., p. 58-59.
4. Hardy, G.H. and E.M. Wright (2008). *An Introduction to the Theory of Numbers*, Sixth Edition. Oxford, UK: Oxford University Press, p. 58-59.
5. Shanks, p. 22-23.
6. Hardy, G.H. and E.M. Wright, p. 3-4.
7. Wells, p. 188.
8. Shanks, p. 204-205.
9. Beeler, Robert A., (2015). *How to Count*. New York: Springer, p. 21.
10. Apostol, Tom M., (1976). *Introduction to Analytic Number Theory*. New York: Springer, p. 27-28.
11. Beeler, p. 9.
12. Beeler, p. 195
13. Shanks, p. 69.