Proofs Regarding Primorial Patterns

by

Dennis R. Martin
DP Technology Corp., Camarillo, CA
dennis.martin@dptechnology.com
BSME, Michigan Technological University, Houghton, MI
Department of Mathematics, University of California, Santa Barbara
drmartin@umail.ucsb.edu

This document is available in other formats. See www.primenace.com.

Abstract

Observations are made regarding the pattern of the composite numbers that have a particular prime factor for their lowest prime factor. It is subsequently proven that this pattern repeats over intervals equal to the primorial of that lowest prime factor such that the number and distribution of such composites is constant. The value of that constant composite to primorial ratio is proven to be related to the previous prime numbers and its constant composite to primorial ratio.

1 Introduction

It seems well known that the pattern of composite numbers repeats with a period equal to the primorial of each prime factor. Dickson [1] refers to remarks by H.J.S Smith in 1857 and papers by J. DeChamps published in 1907 regarding this property, and Weisstein [2] makes note of it. However, actual proofs of these properties do not seem to be readily available. This paper attempts to rectify that situation by starting from the ground up and deriving some general relationships and developing proofs based on them.

2 Singular Identities

A **prime number** is a number greater than 1 that has no positive integer divisors other than 1 and itself.[3] By the **fundamental theorem of arithmetic**, every positive integer greater than 1 can be uniquely represented by its prime divisors in what is called a **prime factorization**.[4, 5] Since a prime p_N has no other positive integer divisors besides 1 and itself, the prime factorization of p_N is simply p_N. A positive integer greater than 1 which is not prime is a **composite number**.[6]

By convention the number 1 is considered neither prime nor composite. Every positive integer greater than 1 is either a prime number or a composite number. For every positive integer greater than 1, then, one of the following statements must be true:

1. The prime p_N is a factor in its prime factorization.
2. The prime p_N is not a factor in its prime factorization.

If a number n has a prime factorization where p_N is a single factor, that is p_N^i is a factor and $i = 1$, and if p_N^1 is the only factor other than 1, then $n = p_N$ and it is prime. Otherwise it is a composite number which we can label C.

Lemma 1: For every composite number C having p_N as a factor, one of the following statements must be true:

1. The **lowest prime factor** of C is smaller than p_N. That is, p_{N-J} is the lowest prime factor and $p_{N-J} < p_N$.
2. The lowest prime factor is p_N and it is the lone prime factor, i.e. $p_N^i = C$ where $i \geq 2$.
3. p_N is the lowest prime factor while the other factor is a larger prime $p_{N+J} > p_N$ or a product of one or more larger primes such as $(p_{N+J})^k$ or $(p_{N+J}) \bullet (p_{N+L})$ or combinations of their higher powers.

Proof: If p_N is a factor by itself, then it is of the form p_N^i, but i cannot be 1 because then the number would be prime, so i must be greater than 1 and thus satisfy condition 2. If p_N is not a factor by itself, then it must be combined with at least one other prime. If any of the other primes in the prime factorization is less than p_N then condition 1 is satisfied, otherwise all of them must be greater than p_N, in which is the case covered by condition 3.

Q.E.D.

3 Primorial Soup

The **primorial** is analogous to a factorial applied to the sequence of prime numbers.[7] The primorial for the prime p_N is the product of all primes up to and including p_N, and it is denoted as $p_N\#$. By the definition of factorial, $p_1\# = 2$, and then for every prime greater than 2:

$$p_N\# = p_N \bullet p_{N-1}\# \qquad (1)$$

What happens, though, if instead of just multiplying $p_{N-1}\#$ by p_N to get the next primorial value, we multiply all of the positive integers in the interval up to and including $p_{N-1}\#$ by p_N? What can we say about these numbers, and what about the other integers that we might need to fill in the new interval up to and including $p_N\#$? What would happen if we were to add some multiple of $p_N\#$ onto all of them? What can we say about the lowest prime factors of those numbers?

For example, start with the number 1, and multiply it by the first prime $p_1 = 2$. We now have an interval the width of the primorial $p_1\# = 2$ containing the numbers 1 and 2. Add any multiple of 2 onto these two numbers. That is, let n be a non-negative integer where $n = 0, 1, 2, 3, 4, 5\ldots$ The result of the addition is an interval of width $p_1\# = 2$ containing the numbers $2n + 1$ and $2n + 2$. For those numbers, the statements that follow, where ≡ indicates **congruence**, are always true.[8]

$$(2n + 1) \equiv 1 \pmod 2$$
$$(2n + 2) \equiv 0 \pmod 2$$

Therefore within every interval of width $p_1\# = 2$ we have one number that has $p_1 = 2$ for its lowest prime factor and another number that does not have 2 for a factor. Except for the case where $n = 0$ and that other number is 1, that other number must either be prime or it must be a composite that has a higher prime $p_{N+J} > p_1$ for its lowest prime factor. Essentially we have just found that every even number is evenly divisible by 2 and that every odd number is not.

Now take that first primorial and multiply it by the second prime, $p_2 = 3$ and fill in the spaces in between. The result is an interval of width $p_2\# = 6$ containing the numbers 1, 2, 3, 4, 5, 6. Add any multiple of 6 on to those numbers. The result will be an interval the width of the primorial $p_2\# = 6$, still, containing the following numbers:

$$(6n + 1), (6n + 2), (6n + 3), (6n + 4), (6n + 5), (6n + 6)$$

Let us factor these values. While we could factor a 3 from out of two of those numbers, though, let us instead only factor the lowest prime factor possible out of each. This factoring produces:

$$(6n + 1) \equiv 1 \pmod 6$$
$$2 \bullet (3n + 1) \equiv 2 \pmod 6 \equiv 0 \pmod 2$$
$$3 \bullet (2n + 1) \equiv 3 \pmod 6 \equiv 0 \pmod 3$$

$2 \bullet (3n + 2) \equiv 4 \pmod 6 \equiv 0 \pmod 2$
$(6n + 5) \equiv 5 \pmod 6$
$2 \bullet (3n + 3) \equiv 0 \pmod 6 \equiv 0 \pmod 2$

Performing a **lowest prime factorization** like this allows us to more easily count the numbers within the primorial interval in terms of their lowest prime factor.

Out of every $p_2\#$ primorial interval, we can see that there are three numbers that have 2 for their lowest prime factor, one number that has 3 for its lowest prime factor (the $3 \bullet (2n + 1)$ term), and two other numbers which do not have 2 or 3 as a factor at all. That there are three numbers that have 2 for their lowest prime factor makes sense because we multiplied the previous primorial by 3 and that primorial interval had one number that had 2 for its lowest prime factor. But notice also that the term that does have 3 for its lowest prime factor has the same form as the term that did *not* have 2 as a factor in that previous $p_1\#$ primorial interval. That is:

$$(2n + 1) \equiv 1 \pmod 2 \quad \rightarrow \quad 3 \bullet (2n + 1) \equiv 3 \pmod 6 \equiv 0 \pmod 3$$

To summarize what can be concluded so far:

a. 1 out of every 2 and 3 out of every 6 numbers have 2 for their lowest prime factor.
b. 1 out of every interval of 6 numbers has 3 for its lowest prime factor.
c. 4 numbers total out of every 6 have either 2 or 3 for their lowest prime factor.
d. 2 out of every 6 numbers do not have 2 or 3 as a factor. Ignoring the trivial case where one of those is 1, those two numbers individually are either prime or have a prime that is higher than 3 for their lowest prime factor.

The count in (d) can be calculated as the primorial value minus the count from (a) that have 2 for their lowest prime factor minus the count from (b) that has 3 for its lowest prime factor. But the count from (a) corresponds back to the count in the $p_1\# = 2$ interval that had 2 for a lowest prime factor and the count from (b) matches the count from the previous $p_1\# = 2$ interval which did not have 2 as a factor. Thus the count in (d) is directly related to counts in the previous primorial.

4 A Preliminary Proof by Induction

By induction then, if we multiply the first interval of 6 by $p_3 = 5$ and then add any multiple of $p_3\# = 5 \bullet 6 = 30$, we should expect the three numbers that had 2 as their lowest prime factor in the previous $p_2\# = 6$ primorial to lead to $3 \bullet 5 = 15 = 30 / 2$ which have 2 as their lowest prime factor in each $p_3\# = 30$ primorial interval. We should also expect the one that had 3 as its lowest prime factor in the previous to lead to $1 \bullet 5 = 5 = 30 / 6$ that have 3 as their lowest prime factor in this interval, and the 2 that had neither 2 nor 3 as a factor should now relate to two composites that have 5 for their lowest prime factor. That will leave $30 – 15 – 5 – 2 = 8$ that have do not have 2, 3 or 5 as a factor. If not equal to 1, then each of those eight must either be prime themselves or must have a prime higher than 5 as their lowest prime factor.

Let us set about proving what has been implied by induction. Take the first 30 positive integers and add any multiple of $p_3\# = 30$ onto them. The result is a set having the values {(30*n* + 1), (30*n* + 2), (30*n* + 3), (30*n* + 4), (30*n* + 5), (30*n* + 6), …(30*n* + 29), (30*n* + 30)}. Now factor the lowest prime factor possible out of each of them. The results of this lowest prime factorization including various relevant **residues** are shown in Table 1.

Table 1: Lowest Prime Factorization of Any Multiple of the $p_3\# = 5\# = 30$ Primorial Interval

Primorial Interval Member	Lowest Prime Factorization	Residues		
		Modulo $p_3\#$	Modulo $p_2\#$	Modulo Lowest p_N
30*n* + 1	(30*n* + 1)	1 (mod 30)	1 (mod 6)	
30*n* + 2	2 • (15*n* + 1)	2 (mod 30)	2 (mod 6)	0 (mod 2)
30*n* + 3	3 • (10*n* + 1)	3 (mod 30)	3 (mod 6)	0 (mod 3)
30*n* + 4	2 • (15*n* + 2)	4 (mod 30)	4 (mod 6)	0 (mod 2)
30*n* + 5	**5 • (6*n* + 1)**	**5 (mod 30)**	**5 (mod 6)**	**0 (mod 5)**
30*n* + 6	2 • (15*n* + 3)	6 (mod 30)	0 (mod 6)	0 (mod 2)
30*n* + 7	(30*n* + 7)	7 (mod 30)	1 (mod 6)	
30*n* + 8	2 • (15*n* + 4)	8 (mod 30)	2 (mod 6)	0 (mod 2)
30*n* + 9	3 • (10*n* + 3)	9 (mod 30)	3 (mod 6)	0 (mod 3)
30*n* + 10	2 • (15*n* + 5)	10 (mod 30)	4 (mod 6)	0 (mod 2)
30*n* + 11	(30*n* + 11)	11 (mod 30)	5 (mod 6)	
30*n* + 12	2 • (15*n* + 6)	12 (mod 30)	0 (mod 6)	0 (mod 2)
30*n* + 13	(30*n* + 13)	13 (mod 30)	1 (mod 6)	
30*n* + 14	2 • (15*n* + 7)	14 (mod 30)	2 (mod 6)	0 (mod 2)
30*n* + 15	3 • (10*n* + 5)	15 (mod 30)	3 (mod 6)	0 (mod 3)
30*n* + 16	2 • (15*n* + 8)	16 (mod 30)	4 (mod 6)	0 (mod 2)
30*n* + 17	(30*n* + 17)	17 (mod 30)	5 (mod 6)	
30*n* + 18	2 • (15*n* + 9)	18 (mod 30)	0 (mod 6)	0 (mod 2)

$30n + 19$	$(30n + 19)$	19 (mod 30)	1 (mod 6)	
$30n + 20$	$2 \bullet (15n + 10)$	20 (mod 30)	2 (mod 6)	0 (mod 2)
$30n + 21$	$3 \bullet (10n + 7)$	21 (mod 30)	3 (mod 6)	0 (mod 3)
$30n + 22$	$2 \bullet (15n + 11)$	22 (mod 30)	4 (mod 6)	0 (mod 2)
$30n + 23$	$(30n + 23)$	23 (mod 30)	5 (mod 6)	
$30n + 24$	$2 \bullet (15n + 12)$	24 (mod 30)	0 (mod 6)	0 (mod 2)
$30n + 25$	**$5 \bullet (6n + 5)$**	**25 (mod 30)**	**1 (mod 6)**	**0 (mod 5)**
$30n + 26$	$2 \bullet (15n + 13)$	26 (mod 30)	2 (mod 6)	0 (mod 2)
$30n + 27$	$3 \bullet (10n + 9)$	27 (mod 30)	3 (mod 6)	0 (mod 3)
$30n + 28$	$2 \bullet (15n + 14)$	28 (mod 30)	4 (mod 6)	0 (mod 2)
$30n + 29$	$(30n + 29)$	29 (mod 30)	5 (mod 6)	
$30n + 30$	$2 \bullet (15n + 15)$	0 (mod 30)	0 (mod 6)	0 (mod 2)

As expected there are 15 numbers within each interval of 30 that have 2 as their lowest prime factor. All of them relate to a value within a primorial interval of the previous prime. That is, all of them are congruent to either 2 or 4 or 0 (mod 6).

There are 5 numbers within each interval of 30 that have 3 as their lowest prime factor. Those 5 relate to a specific value within a primorial interval of $p_2\# = 6$ in that all of them have a residue of 3 (mod 6).

Then there are 2 numbers (as highlighted in bold in Table 1) within each interval of 30 that have 5 as their lowest prime factor. Those two are directly related to the two factors that did not have 2 or 3 as a factor within the primorial of the previous prime. They are the values with residues of 1 (mod 6) and 5 (mod 6):

$$(6n + 1) \equiv 1 \pmod{6} \quad \rightarrow \quad 5 \bullet (6n + 1) \equiv 1 \pmod{6} \equiv 0 \pmod{5}$$
$$(6n + 5) \equiv 5 \pmod{6} \quad \rightarrow \quad 5 \bullet (6n + 5) \equiv 5 \pmod{6} \equiv 0 \pmod{5}$$

Finally that leaves 8 numbers within each interval of 30 that do not have 2, 3, or 5 as a factor. The results for the primorial $p_3\# = 30$ match what we predicted by induction from $p_2\#$. Let us now generalize this as a theorem and prove it for any primorial.

5 Deriving the General Theorems

Theorem 1: Over any interval equal to the primorial $p_N\#$ of a particular prime p_N, the count of the numbers having p_N as their lowest prime factor is constant, as is the count of the numbers having any prime p_{N-J} that is less than p_N as their lowest prime factor a constant as well.

Proof: Let the sequence of numbers a_0, a_1, a_2, … a_{m-2}, a_{m-1} represent all of the integers within any interval of the primorial $p_N\#$ such that $a_i \in \{a\}$ and $(n \bullet p_N\# + A) < a_i \leq ((n + 1) \bullet p_N\# + A)$, where n is a non-negative integer and A is an integer offset. Since we are only concerned with prime factors, and 1 has no prime factors, let us also stipulate that $1 \leq A \leq p_N\#$ so that all $a_i > 1$.

Divide every integer in the interval by the primorial value. Since every integer is unique, each one will have a unique residue with respect to the primorial. That is, each will produce an integer residue going from 0 up to the primorial value minus 1 with the primorial as the **modulus**.

$$p_N\# \mid \{a\} \qquad \rightarrow \qquad [\ \equiv \{0, 1, 2, 3 \ldots (p_N\# - 2), (p_N\# - 1)\} \pmod{p_N\#}\ ]$$

The entity on the right is a residue system. Because each integer value from zero up to the modulus minus 1 is represented as a residue, this is a **complete residue system**.[9]

Label this residue system $\{r\}_N$. Since the primorial is a factorial product of the previous lower primes, let us divide those residues by the primorial value of the next lower prime. Since each residue is unique within the range from 0 up to the original primorial, each new residue with respect to the primorial of the previous prime will be unique within an interval of that primorial, and the number of subintervals of that primorial will be equal to the value of the original prime p_N that we started with. Thus each lower residue system with the lower primorial value as the modulus will be repeated a number of times equal to the value of that original, next higher prime.

$$p_{N-1}\# \mid \{a\} \qquad \rightarrow \qquad [\ \equiv \{0, 1, 2, 3 \ldots (p_{N-1}\# - 2), (p_{N-1}\# - 1)\} \pmod{p_{N-1}\#}\ ]\ \mathbf{x}\ p_N$$

Label the new residue system in brackets as $\{r\}_{N-1}$. There are p_N of these $\{r\}_{N-1}$ residue systems within each $p_N\#$ primorial, and each of them is a complete residue system. We can continue by dividing all of these residue systems by $p_{N-2}\#$ to produce the $\{r\}_{N-2}$ system in brackets below:

$$p_{N-2}\# \mid \{a\} \qquad \rightarrow \qquad [\ \equiv \{0, 1, 2, 3 \ldots (p_{N-2}\# - 2), (p_{N-2}\# - 1)\} \pmod{p_{N-2}\#}\ ]\ \mathbf{x}\ (p_N \bullet p_{N-1})$$

There are $(p_N \bullet p_{N-1})$ of these $\{r\}_{N-2}$ residue systems within the original $p_N\#$ primorial. This process can continue all the way down to $p_1\# = 2$, where the complete residue system labeled $\{r\}_1$ is $[\ \equiv \{0, 1\} \pmod 2\ ]$. There would be $(p_N \bullet p_{N-1} \bullet p_{N-2} \bullet \ldots \bullet p_2) = (p_N\# / 2)$ of these $\{r\}_1$ residue systems within an interval of $p_N\#$.

We can use $\{r\}^N{}_L$ to represent the count of complete residue systems $\{r\}_L$ that have for their modulus the primorial $p_L\#$ of a lower prime $p_L < p_N$ within an interval of the primorial $p_N\#$.

$$\{r\}^{N}{}_{L} = p_N\# / p_L\# \qquad (2)$$

There is always just one complete residue system $\{r\}_N$ within an interval of $p_N\#$, thus $\{r\}^{N}{}_{N} = 1$, and there would be $(p_N\# / p_1\#) = (p_N\# / 2) = \{r\}^{N}{}_{1}$ instances of the $\{r\}_1$ residue system within $p_N\#$. All of the values from the original $p_N\#$ primorial interval that are congruent to 0 (mod 2) have $p_1 = 2$ as their lowest prime factor. There would be $(p_N\# / 2) = \{r\}^{N}{}_{1}$ such values. Only those values that are congruent to 1 (mod 2) can have a higher prime number $p_H > p_1$ as their lowest prime factor.

Let ρ_N represent the ratio of numbers within the primorial for p_N that have p_N as their lowest prime factor. There is only one value that is congruent to 0 (mod 2) in each interval of $p_1\# = 2$, therefore $\rho_1 = 1$. That means that there is always one number in each interval of 2 that is not a multiple of 2. That is the value that is congruent to 1 (mod 2) and its count can be calculated as $p_1\# - \rho_1 = 2 - 1 = 1$. Theorem 1 definitely applies to the first prime and its primorial.

For an interval of $p_2\# = 6$, the residue system $\{r\}_2$ contains {0, 1, 2, 3, 4, 5} (mod 6). There must be $\rho_1 \bullet \{r\}^{2}{}_{1} = \rho_1 \bullet (p_2\# / p_1\#) = 3$ numbers within that interval that have 2 as their lowest prime factor. Those three are congruent to {0, 2, 4} (mod 6). Another way to think of this is that, since initially multiplying the primorial of 2 by $p_2 = 3$ generates the primorial of 6, there must be three multiples of 2 within that 6, because there is always one multiple of 2 within each interval of 2.

When the value congruent to 0 (mod 2) in an interval of 2 is multiplied by 3 in generating an interval of 6, the result is congruent to 0 (mod 6) and since 6 is divisible by 2, it is still congruent to 0 (mod 2). An even number times any positive integer is always an even number. So while there are two multiples of 3 in each interval of 6, one of them must have 2 as its lowest prime factor. The other one corresponds back to a value that was congruent to 1 (mod 2) in the interval of 2, the count of which was $p_1\# - \rho_1$. When it is multiplied by 3 the result is congruent to 3 (mod 6) and hence to 0 (mod 3). That there is one such value means $\rho_2 = 1 = p_1\# - \rho_1$.

The count of what is left, then, is $p_2\# - \rho_1 \bullet (p_2\# / p_1\#) - \rho_2 = 6 - 3 - 1 = 2$. There are two numbers in each multiple of 6 that do not have 2 or 3 as their lowest prime factor. They are the numbers congruent to 1 or 5 (mod 6). Those numbers are each either a composite that has a prime greater than p_2 as their lowest prime factor or they themselves are prime. When an interval of 6 is multiplied by $p_3 = 5$ to initially generate an interval of $p_3\# = 30$, it is these two values and only these two values that can produce composites that have 5 as their lowest prime factor.

The other four numbers in the interval of 6 will, when multiplied by 5, result in composites that still have 2 or 3 as a prime factor. This implies that $\rho_3 = 2 = p_2\# - \rho_1 \bullet (p_2\# / p_1\#) - \rho_2$.

Since $p_2\# = p_2 \bullet p_1\#$, we can factor p_2 from the first two terms on the right side of that expression:

$$\rho_3 = p_2 \bullet (p_1\# - \rho_1 \bullet (p_1\# / p_1\#)) - \rho_2 = p_2 \bullet (p_1\# - \rho_1) - \rho_2$$

But $\rho_2 = (p_1\# - \rho_1)$, so substituting yields:

$$\rho_3 = p_2 \bullet \rho_2 - \rho_2 = \rho_2 \bullet (p_2 - 1) = 1 \bullet (3 - 1) = 2$$

An interval of $p_3\# = 30$ would contain $\{r\}^3{}_1 = (p_3\# / p_1\#) = 15$ instances of the $\{r\}_1$ residue system, $\{r\}^3{}_2 = (p_3\# / p_2\#) = 5$ instances of the $\{r\}_2$ residue system, and of course $\{r\}^3{}_3 = (p_3\# / p_3\#) = 1$ instance of the $\{r\}_3$ residue system. Thus there would be $\rho_1 \bullet \{r\}^3{}_1 = 15$ numbers that have 2 as their lowest prime factor, $\rho_2 \bullet \{r\}^3{}_2 = 5$ numbers that have 3 as their lowest prime factor, and $\rho_3 \bullet \{r\}^3{}_3 = 2$ numbers that have 5 as their lowest prime factor. The numbers that are left do not have 2, 3, or 5 as a factor. When this interval of $p_3\# = 30$ is multiplied by $p_4 = 7$ to generate an interval of $p_4\# = 210$, it is these numbers that will have $p_4 = 7$ as their lowest prime factor:

$$\rho_4 = p_3\# - \rho_1 \bullet \{r\}^3{}_1 - \rho_2 \bullet \{r\}^3{}_2 - \rho_3 \bullet \{r\}^3{}_3 = p_3\# - \Sigma\, (\rho_L \bullet \{r\}^3{}_L) \qquad \{\text{for } L = 1 \text{ to } 3$$

In this case, $\rho_4 = 30 - 15 - 5 - 2 = 8$. The factorization of those 8 numbers is shown in Table 2.

Table 2: Factorization of Any $p_4\# = 210$ Primorial Interval for the Lowest Prime Factor $p_4 = 7$

Primorial Interval Member	Lowest Prime Factorization	Residues		
		Modulo $p_4\#$	Modulo $p_3\#$	Modulo $p_2\#$
$210n + 7$	$7 \bullet (30n + 1)$	7 (mod 210)	1 (mod 30)	1 (mod 6)
$210n + 49$	$7 \bullet (30n + 7)$	49 (mod 210)	7 (mod 30)	1 (mod 6)
$210n + 77$	$7 \bullet (30n + 11)$	77 (mod 210)	11 (mod 30)	5 (mod 6)
$210n + 91$	$7 \bullet (30n + 13)$	91 (mod 210)	13 (mod 30)	1 (mod 6)
$210n + 119$	$7 \bullet (30n + 17)$	119 (mod 210)	17 (mod 30)	5 (mod 6)
$210n + 133$	$7 \bullet (30n + 19)$	133 (mod 210)	19 (mod 30)	1 (mod 6)
$210n + 161$	$7 \bullet (30n + 23)$	161 (mod 210)	23 (mod 30)	5 (mod 6)
$210n + 203$	$7 \bullet (30n + 29)$	203 (mod 210)	29 (mod 30)	5 (mod 6)

The count of the numbers that do not have a prime p_N or lower as their lowest prime factor within an interval of $p_N\#$ represents the count of the numbers that will have p_{N+1} as their lowest prime factor in an interval of $p_N\# \bullet p_{N+1} = p_{N+1}\#$. The previous expression can be generalized as:

$$\rho_{N+1} = p_N\# - \Sigma\, (\rho_L \bullet \{r\}^N{}_L) \quad \{\text{for } L = 1 \text{ to } N \qquad (3)$$

From equation (2) we have $\{r\}^{N}_{L} = p_N\# / p_L\#$, and from equation (1) we have $p_N\# = p_N \bullet p_{N-1}\#$, so p_N can be factored from all of the terms on the right of equation (3) similar to what was done with ρ_3, which leads to $\rho_{N+1} = \rho_N \bullet (p_N - 1)$, or alternatively, with N > 1:

$$\rho_N = \rho_{N-1} \bullet (p_{N-1} - 1) \qquad (4)$$

Thus ρ_N is a constant for all $p_N\#$ intervals. Solving equation (4) for ρ_4 gives $\rho_4 = \rho_3 \bullet (p_3 - 1) = 2 \bullet (5 - 1) = 8$, which is in agreement with what we arrived at previously. Not only have we proven that ρ_N is a constant, but we have proven that it is related to previous values of ρ.

Q.E.D.

This relationship also corresponds to the local minima of Euler's totient (phi) function and appears in the On-Line Encyclopedia of Integer Sequences as A005867.[10]

Obviously there are no numbers less than p_N that can have p_N as a factor, and since p_N itself is prime, it is not necessary to consider any primorial intervals that start at p_N or lower. It is the intervals that start at $p_N + 1$ and above that are important. In those intervals, the numbers represented by ρ_N all must be composite; therefore we can refer to ρ_N as the **composite to primorial ratio**. The interval that starts at $p_N + 1$ would complete its first full primorial interval at $p_N + p_N\#$. Because in some ways we can think of composite numbers as molecules composed of their constituent prime factor atoms and arranged in a lattice across their primorial interval, this value shall be called the **first atomic boundary** and labeled α_N. If we make a function $T_N(x)$ to count the number of composites that have p_N as their lowest prime factor, then we can say that $\rho_N = T_N(\alpha_N)$. Table 3 lists these values for the first twelve primes.

Table 3: Composite to Primorial Ratio and Ratio Summation for the First Twelve Primes

N	p_N	$p_N\#$	$\alpha_N = p_N\# + p_N$	$\rho_N = T_N(\alpha_N)$	Σ (Numerator)
1	2	2	4	1	1
2	3	6	9	1	4
3	5	30	35	2	22
4	7	210	217	8	162
5	11	2310	2321	48	1830
6	13	30030	30043	480	24270
7	17	510510	510527	5760	418350
8	19	9699690	9699709	92160	8040810

9	23	223092870	223092893	1658880	186597510
10	29	6469693230	6469693259	36495360	5447823150
11	31	200560490130	200560490161	1021870080	169904387730
12	37	7420738134810	7420738134847	30656102400	6317118448410

Now that we have a proof that the count of the numbers having p_N as their lowest prime factor is constant over any interval of $p_N\#$, what can we say about the pattern of those numbers?

Theorem 2: The pattern of the numbers having p_N as their lowest prime factor repeats over intervals of the primorial $p_N\#$.

Proof: Again let the sequence of numbers a_0, a_1, a_2, … a_{m-2}, a_{m-1} represent all the integers within any interval of the primorial $p_N\#$ such that $a_i \in \{a\}$ and $(n \bullet p_N\# + A) < a_i \leq ((n + 1) \bullet p_N\# + A)$, where n is a non-negative integer and A is an integer offset where $1 \leq A \leq p_N\#$ so that all $a_i > 1$.

When the primorial $p_N\#$ is divided into $\{a\}$, the resulting residue system $\{r\}_N$ is a complete residue system. This means that each residue r_i in $\{r\}_N$ can be mapped to exactly one of the integers in $\{a\}$. Map the residue $r_0 = 0$ to a_0, and the residue $r_1 = 1$ to a_1, and so on, up to $r_{m-1} = \mathrm{m} - 1$, which maps to a_{m-1}. The result of this mapping is that $a_i \equiv \mathrm{i} \pmod{p_N\#}$ for all i where $0 \leq \mathrm{i} \leq \mathrm{m} - 1$ and where m represents the modulus $p_N\#$ so that $\mathrm{m} - 1 = p_N\# - 1$.

Let $n = n + 1$ so that a new sequence $\{a'\}$ is generated for the next primorial interval. That is, let a_0', a_1', a_2', … a_{m-2}', a_{m-1}' represent all the integers within the next primorial interval such that $((n + 1) \bullet p_N\# + A) < a_i' \leq ((n + 2) \bullet p_N\# + A)$ for all a_i'.

This means that a_i¢ $= a_i + p_N\#$ for all i where again $0 \leq \mathrm{i} \leq \mathrm{m} - 1$ and $\mathrm{m} - 1 = p_N\# - 1$. Since $a_i \equiv \mathrm{i} \pmod{p_N\#}$ for all i and $p_N\# \equiv 0 \pmod{p_N\#}$, this implies that a_i¢ $\equiv \mathrm{i} \pmod{p_N\#}$ for all i, meaning that the residues for the next primorial interval can be mapped to the integers within the primorial in the exact same order every time.

As shown in the proof of theorem 1, the numbers that have p_N as their lowest prime factor have residue modules the primorial $p_N\#$ that relates to a specific residue in the previous $p_{N-1}\#$ primorial. For example, the numbers that are 0 (mod 5) within a primorial of 5# = 30 and thus have $p_3 = 5$ for their lowest prime factor have residues of 1 or 5 (mod 6). Since those residues are mapped in the same order for every interval, the numbers that have p_N as their lowest prime factor occur in the same order in every interval as well. This can easily be seen in Table 1 where the residues modulo $p_3\# = 30$ would repeat in the same order for the next $n + 1$ interval.

Q.E.D.

Theorem 3: The pattern of the numbers having p_N as their lowest prime factor is symmetrical within intervals of the primorial $p_N\#$.

Proof: Again let the sequence of numbers a_0, a_1, a_2, … a_{m-2}, a_{m-1} represent all the integers within any interval of the primorial $p_N\#$ such that $a_i \in \{a\}$ and $(n \bullet p_N\# + A) < a_i \leq ((n + 1) \bullet p_N\# + A)$, where n is a non-negative integer and A is an integer offset where $1 \leq A \leq p_N\#$ so that all $a_i > 1$.

Then once again divide the primorial $p_N\#$ into $\{a\}$ and map the resulting residues $r_0 = 0$ to a_0, and $r_1 = 1$ to a_1, and so on, up to $r_{m-1} = m - 1$ to a_{m-1}, such that $a_i \equiv i \pmod{p_N\#}$ for all i.

Now pair up the members of the interval based on the residues. Pair a_0 with a_{m-1}, a_1 with a_{m-2}, and so on, such that for each pair (a_j, a_k) the sum $j + k = m - 1$. Since $a_j \equiv j \pmod{p_N\#}$ and $a_k \equiv k \pmod{p_N\#}$, then by the properties of congruence, $(a_j + a_k) \equiv (j + k) \pmod{p_N\#} \equiv (m - 1) \pmod{p_N\#}$.[11] Since $m - 1 = p_N\# - 1$, that is equivalent to saying $(a_j + a_k) \equiv (-1) \pmod{p_N\#}$.

Now suppose we pair up the members of the interval again, but this time pair a_0 with a_1, then a_2 with a_{m-1}, and a_3 with a_{m-2}, and so on, such that for each pair (a_j, a_k) either the sum $j + k = 1$ or the sum $j + k = m + 1$. Since m represents the modulus $p_N\#$, that is equivalent to saying $(a_j + a_k) \equiv 1 \pmod{p_N\#}$.

Likewise it is possible to produce pairs (a_j, a_k) for every residue r_i in the original complete residue system so that $(a_j + a_k) \equiv r_i \pmod{p_N\#}$. We can say that the residue system $\{r\}$ is invariant under this pair-wise transformation.

We can also invert the residue system by subtracting each a_i from $((n + 1) \bullet p_N\# + A) + 1$ to generate a new sequence {a¢}. Dividing the primorial $p_N\#$ into {a¢} will result in the complete residue system {r¢}, where r_i¢ = m – r_i. For example, we previously noted that an interval for the primorial $p_2\# = 6$ contains the values $(6n + 1)$, $(6n + 2)$, $(6n + 3)$, $(6n + 4)$, $(6n + 5)$, and $(6n + 6)$ which produces the residue system $\{1, 2, 3, 4, 5, 0\} \pmod 6$. Subtract these values from $(6n + 7)$ and the results are the values 6, 5, 4, 3, 2, 1 which produces the residue system $\{0, 5, 4, 3, 2, 1\} \pmod 6$, which is the inverse of the original residue system. So we can also say that the residue system $\{r\}$ is invariant under inversion.

That $\{r\}$ is invariant under these transformations allows us to conclude that the pattern is symmetrical. That symmetry can readily be seen in Table 1.

Q.E.D.

Conclusions

The technique of characterizing composites by their lowest prime factor over primorial intervals potentially has several useful applications. It is hoped that these proofs can help in the development of such applications.

Acknowledgments

I am grateful to the following individuals for their assistance and advice: Dr. Peter Gibson, The University of Alabama in Huntsville; Dr. Charles Ryavec and Dr. Jeffrey Stopple, University of California, Santa Barbara; Kaustuv M. Das and Joseph Paunovich of DWT. And finally a special thanks to DP Technology Corp. and its management for their support and encouragement.

References:

1. Dickson, Leonard E. "History of the Theory of Numbers Volume I: Divisibility and Primality". Mineola, NY: Dover Publications, Inc., 2005, p. 439.

2. Weisstein, Eric W. "Twin Peaks." From *MathWorld*--A Wolfram Web Resource. http://mathworld.wolfram.com/TwinPeaks.html

3. Eric W. Weisstein. "Prime Number." From *MathWorld*--A Wolfram Web Resource. http://mathworld.wolfram.com/PrimeNumber.html

4. Eric W. Weisstein. "Fundamental Theorem of Arithmetic." From *MathWorld*--A Wolfram Web Resource. http://mathworld.wolfram.com/FundamentalTheoremofArithmetic.html

5. Eric W. Weisstein. "Prime Factorization." From *MathWorld*--A Wolfram Web Resource. http://mathworld.wolfram.com/PrimeFactorization.html

6. Eric W. Weisstein. "Composite Number." From *MathWorld*--A Wolfram Web Resource. http://mathworld.wolfram.com/CompositeNumber.html

7. Eric W. Weisstein. "Primorial." From *MathWorld*--A Wolfram Web Resource. http://mathworld.wolfram.com/Primorial.html

8. Eric W. Weisstein. "Congruence." From *MathWorld*--A Wolfram Web Resource. http://mathworld.wolfram.com/Congruence.html

9. Eric W. Weisstein. "Complete Residue System." From *MathWorld*--A Wolfram Web Resource. http://mathworld.wolfram.com/CompleteResidueSystem.html

10. Sloane, N. J. A. Sequence A005867 in "The On-Line Encyclopedia of Integer Sequences."

11. Eric W. Weisstein. "Congruence." From *MathWorld*--A Wolfram Web Resource. http://mathworld.wolfram.com/Congruence.html

Bibliography:

Caldwell, Chris K. “The Prime Pages”, http://primes.utm.edu/.

Crandall, R. and Pomerance, C. *Prime Numbers: A Computational Perspective, 2nd ed.* New York: Springer-Verlag, 2005.

Dickson, Leonard E. “History of the Theory of Numbers Volume I: Divisibility and Primality”. Mineola, NY: Dover Publications, Inc., 2005.

Guy, Richard K. “Unsolved Problems in Number Theory, Third Edition”. New York: Springer-Verlag, 2005.

Riesel, H. *Prime Numbers and Computer Methods for Factorization, 2nd ed.* Boston, MA: Birkhäuser, 1994.