A Fundamental Therorem Of Prime Sieving

Russell Letkeman
r. letkeman@gmail. com

Dedicated to my son Panha

July 29, 2014

Abstract

We introduce a fundamental theorem of prime sieving *(FTPS)* and show how it illuminates structure on numbers co-prime to a random product of unique prime numbers. This theorem operates on the transition between the set of numbers co-prime to any product of unique prime numbers and the new set when another prime number is introduced in the product.

We use this to develop tools which exactly count certain gap n-tuples in sets modulo a unique product of prime numbers.

1 Notation

Let P_m be the m^{th} prime with the usual ordering $P_m < P_{m+1}$. Though 1 is not prime it is co-prime to every number and we include it as P_0, the *zeroth* prime. We count primes strictly by their index so the usual counting works in the sense that 1 is ignored.

We begin with collections of random primes which we denote as $\{P\}^m$ having m unique prime numbers chosen at random and ordered by size. By insisting on local ordering we induce a local index count, that is we have if $P_a \in \{P\}^m$ and $P_b \in \{P\}^m$ and $P_a < P_b$ than $a < b$. Define their random product as

$$\{P\}^m\# = \prod_{j=1}^{m} P_j$$

If we build our product with the first m consecutive prime numbers, we denote it with the common notation $P_m\#$ without the braces and it is called a primorial.

We also use offset products we call product minors defined as

$$\{P^{-r}\}^m\# = \prod_{j=1}^{m} (P_j - r)$$

with a fixed whole number $r \geq 0$. We are building something akin to a factorial but it is necessarily more complex. If we pre-subtract such a number from a factorial $(n-r)!$

we simply stop our product sooner, for example (10−2)!=8!, and we ignore the last 2 numbers.

In our case, the product minor, we ignore the numbers less than our offset. If all of the prime numbers in the set are less than the offset, than, since every number was ignored in the product the result is undefined or Not A Number. Factorials also have a special property we use, that is (0)!=1. For example $2^{-2}\#$=1. So while $(2{-}2) = 0$, $(2{-}2)\# = 1$.

For example, if our set was $\{P\}^m = \{3, 11, 17, 47\}$ and $r = 11$ than $\{P^{-11}\}^m\# = (17 - 11)(47 - 11)$, while $\{P^{-48}\}^m\# = NaN$. While if $\{P\}^m = \{2, 3, 7, 11\}$ and $r = 11$ than $\{P^{-11}\}^m\# = (11 - 11)\# = 1$.

With the condition that the random primes are consecutive and starting at 2 we will write $\{P\}^m\# = P_m\#$ and we'll write its minors as $P_m^{-r}\#$ and we call it the r^{th} primorial minor.

1.1 Multiplication Modulo A Random Product Of Unique Prime Numbers

Let $n = \{P\}^m\#$, we consider the set of numbers P_j^m co-prime to n. Let ${}^n c_j^m = P_{j+n}^m - P_j^m$ be the n^{th} difference between members. The Euler phi function or totient[1 2] of any such set is

$$\phi\left(\{P\}^m\right) = \{P^{-1}\}^m\#$$

or if we use successive primes beginning at 2 we get

$$\phi\left(P_m\#\right) = P_m^{-1}\#$$

Since each of our sets is bounded, we can define the average n-tuple as

$${}^n c^m = n\frac{\{P\}^m\#}{\{P^{-1}\}^m\#}$$

the result coming from the cyclic nature of modular arithmetic.

We will frequently refer to ${}^0 c^m = \hat{\mathbf{g}}^m$ the average gap and ${}^0 c_j^m = P_{j+1}^m - P_j^m = g_j^m$, the local gap.

1.2 Constructing The Set

We'll use P_j^m to be the j^{th} number co-prime to $\{P\}^m\#$ with P_0^m=1 for every set and $P_j^m < P_{j+1}^m$ being the usual order.

There is no straightforward mechanism short of brute force to find the members given a random random product of prime numbers. However, there is a great deal of simplification available if we build our set first with the smallest prime and systematically multiply the additional primes one at a time.

Beginning with the first prime; P_{a_1}, this forms a set $\{1, 2, 3, 4, \ldots, P_{a_1}{-}1\}$. To cross it with the next prime P_{a_2} which has $P_{a_2}{-}1$ members as well, we first make a hybrid set in matrix form. If $n = P_{a_1}P_{a_2}$

$$h_{ij}^n = P_i^m + jP_{a_1} \;\forall\; j < P_{a_2}$$

We call the stage of building the hybrid set *expansion* for obvious reasons. It is also better written as

$$h^n_{ij} = P^m_i + j\{P\}^m\# \; \forall \, j < P_b, \; m = 1$$

because it doesn't matter how many primes we've actually started with.

The final step is removing $P_a{-}1 = \{P^{-1}\}^k\#$ non co-prime members by identifying them as solutions of

$$P_b P^m_i = P^m_j + n\{P\}^m\# \; \textit{for some } n \textit{ and } j$$

We call the removal of non co-prime members *coalescence* because when a member is removed, the gaps it isolated coalesce into a new gap so total distance is always preserved.

1.3 Said Algebraically

The above can be stated using the totient function, if we have a set made from $\{P\}^m\#$ with $\{P^{-1}\}^m\#$ members, and we multiply in a new prime P_{m+1} we first generate a hybrid set with $P_z\{P^{-1}\}^m\#$ and remove $\{P^{-1}\}^m\#$ non co-prime members leaving $\{P^{-1}\}^{m+1}\#$ members. Or if we used consecutive primes beginning with 2 we get

$$P^{-1}_{m+1}\# = P_{m+1}P^{-1}_m\# - P^{-1}_m\#$$

1.4 Said Mechanically

For a concrete example we'll choose $\{3, 5\}$ and begin with the set

$$3 = \left\{\begin{matrix} 1 & 2 \\ 1 & 2 \\ 3 & 3 \end{matrix}\right\} * 5 = \left\{\begin{matrix} 1 & 2 \\ 4 & \underline{5} \\ 7 & 8 \\ \underline{10} & 11 \\ 13 & 14 \end{matrix}\right\}$$

where we have underlined the non co-prime members. Once we remove them we get

$$\left\{\begin{matrix} 1 & 2 & 4 & 7 & 8 & 11 & 13 & 14 \\ 1 & 2 & 3 & 1 & 3 & 2 & 1 & 2 \\ 3 & 5 & 4 & 4 & 5 & 3 & 3 & 3 \\ 6 & 6 & 7 & 6 & 6 & 5 & 4 & 5 \\ \vdots & \ddots & & & & & & \end{matrix}\right\}$$

We multiplied our second prime into our first prime. We made 5 rows of 2 each in the hybrid and removed the 2 non co-prime to our new product.

Notice, the non co-prime numbers each occupy a unique column in the hybrid.

1.5 The Theorem

A Fundamental Theorem Of Prime Sieving. *Our fundamental theorem of prime sieving is an observation that the hybrid set has $P_m^{-1}\#$ columns and P_z rows. When the non co-prime members are removed it is such that exactly one member from each $\{P^{-1}\}^m\#$ column is targeted.*

Proof. Assume it's not true, than there exists a pair of numbers in the hybrid such that

$$P_z P_j^m = P_k^m + a\{P\}^m\#$$

and

$$P_z P_l^m = P_k^m + b\{P\}^m\#$$

for $a \; and \; b < P_z$. Assume $P_j^m < P_l^m$ and $a < b$, subtract the 2 equations to get

$$P_z(P_l^m - P_j^m) = (b - a)\{P\}^m\#$$

Now either P_z divides the random product of unique prime numbers not including P_z, which is impossible, or it divides $b - a < P_z$ which is also impossible. □

2 The FTPS And Co-prime Constellations

2.1 Counting Notation

We're going to want to count substructures of gap sets and use the following notation. $T^m_{\{s\}}$ is used to count the occurrence of a particular subsequence of gap types in the set generated by $P_m\#$ in the interval $[1, 1 + P_m\#]$. For example $T^m_{\{2\}}$ counts all the gaps of 2, while $T^m_{\{4,2\}}$ counts all occurrences of gap pairs of $\{4, 2\}$. If it is simply single gaps, we can drop the curly braces and write

$$T^m_{\{2\}} = T^m_2$$

We'll also use a bold font $\mathbf{T}^m_n$ to be the set of all sequences that occur in our interval which sum to the number n.

2.2 Gap Substructures

Since the FTPS guarantees exactly one non co-prime member per column in the hybrid is removed in the finished set, we can ask about how this effects the structure of gap constellations. We'll examine this as if the primes were the standard primorial but the results are quite general.

Consider the following,

$$P_{m+1}P_j^m = P_{k_1}^m + aP_m\#$$

$$P_{m+1}P_{j+1}^m = P_{k_2}^m + aP_m\#$$

subtracting these we get

$$P_{m+1}(P_{j+1}^m - P_j^m) = P_{m+1}g_j^m = P_{k_2}^m - P_{k_1}^m$$

That is, the difference between 2 targets must (of course) be a multiple of the next prime in the product. Also recall, we have the next prime in the product, P_{m+1}, exact copies of the gaps in as many rows forming identical columns of gaps.

Given a gap g_j^m, anchored by 2 numbers co-prime to our product; $P_{j+1}^m - P_j^m = g_j^m$, when we cross in our next larger prime number we have P_z copies; or P_{m+1} if we are using a primorial, forming two consecutive columns represented by

$$P_j^m + aP_m\# \ \forall \ 0 \leq a < P_{m+1}$$

and

$$P_{j+1}^m + bP_m\# \ \forall \ 0 \leq b < P_{m+1}$$

We now ask, how many of the copies survive intact at the next product?

Because of the FTPS, every column of the hybrid must have one hit. So for each such column of gaps, there must be 2 hits that affect it, one anchor to the left and one to the right. And for counting purposes this has only 2 possibilities, $a = b$ or $a \neq b$. There is a single possibility for the case $a = b$ and that comes from our above observation that the gap must be divisible by the new prime number.

That is, there will always be at least $P_{m+1} - 2$ copies of each gap in the new set. That is, most of the new set shares most of its gaps with its progenitor set.

2.3 Twin Gaps And Primorials

If we only consider primorials, we can exactly count twin gaps in every such set.

Theorem 1. *For any integer number n, the interval*

$$[1 + nP_m\#, 1 + (n+1)P_m\#]$$

contains precisely $P_m^{-2}\#$ gaps of size 2. We can also say it has $P_m^{-2}\#$ pairs of numbers co-prime to $P_m\#$ such that $P_{j+1}^m - P_j^m = 2$.

Proof. We only need to show it's true for $n = 1$ or $[1, 1 + P_m\#]$ and the cyclic nature of modular multiplication ensures it will be true for any n.

We begin with $2\#$ which contains exactly 1 gap of 2 in the interval $[1, 1 + 2\#] = [1, 3]$ and we have $(2 - 2)\# = 1$.

Now because every future prime number will be greater than 2, the FTPS says each future generation will have P_{m+1}^{-2} copies of each twin in the progenitor set. We check that $3\#$ has a single twin since

$$(2-2)(3-2)\# = 1$$

and it does as the set $\{1, 5\}$ has corresponding gaps of $\{4, 2\}$.

Now inductively assume it is true for P_m, than that set will have exactly $P_m^{-2}\#$ gaps of 2. Each one of those gaps will have P_{m+1}^{-2} copies in the next set so the set co-prime to $P_{m+1}\#$ will have exactly

$$P_{m+1}^{-2} P_m^{-2}\# = P_{m+1}^{-2}\#$$

gaps of two. □

We can also now make the same claim for gaps of 4, also known as cousin gaps. That is, the count of twin gaps and cousin gaps are identically equal in each interval as long as $P_m > 2$

2.4 Counting Simple Pairs $\{4, 2\}$ And $\{2, 4\}$

In the set generated from 3# we have the gap pair $\{4, 2\}$ occurring once, and we notice $(3 - 3)\# = 1$. Now not any of 2,4 or 6 (their sum), are divisible by any future primes so its count will always be $P_m^{-3}\#$.

The count of $\{2, 4\}$ is exactly the same even if we don't formally see such pairs until 5#. So

$$T_{\{4,2\}}^m = T_{\{2,4\}}^m = P_m^{-3}\# \ \forall \ P > 3$$

References

[1] G. H. Hardy and E. M. Wright 4th Ed. *An Introduction To The Theory Of Numbers.* Oxford University Press, Ely House, London, 1993.

[2] Paulo Ribenboim. *The new Book of Prime Number Records 3rd ed.* Springer Press, Springer-Verlag, New York, Inc., 1995.