INFORMATION

Overview Statement

The pattern in the primes detailed in this work is irrefutable, whilst the various proofs none of which are are used in the pattern derivation, are awaiting formal validation. Please feel free to comment upon the same.

Contact Details

Where you wish to comment or discuss any research or business aspects of the copy-written works, or receive related research pointers, comments and/or letters as attachments may be forwarded by email to dennisleeprimes@gmail.com .

Physics Brief

Advocates of physics, and dark matter, and dark energy, can note that the details provided in section 8, "Quantum Space", provide the introduction of an additional (average of) "6 units" in respect of each atomic element of each of the seven periods in the table of elements. A product factor of 6 delivers an approximation to the sought amount of (invisible) dark matter, and a factor of 6+7=13 delivers the sought amount of dark energy. This implies the possibility of use of the additional "6 units" in current super-string theory, using, for example, a 7-unit real x-axis, and a 6-unit (hyper-complex) y-axis.

Dedication

To my departed father, whose footsteps I walked in, my mentor and guide; my dear mother, who gave me life, and gives me strength; my sweet sister, who in our ignorance is misunderstood; the family remainder, each with differing nuances; the mystery of nature, and the door at the wall; and to those who stopped me in the street and pointed my way.

Copyright and Charge Details

D. LEE B.Sc., M.Res.

The Pattern in the Primes, and Related Results©

or

On Primes, Matrices, and Prime Matrices

A brief dissertation on

Number Theory

by

Dennis Lee B.Sc., M.Res.

Alma Mater

Army Apprentice College Arborfield, Armed Forces, REME

Queen Mary and Westfield College, London

Kings College, London

Strathclyde University, Glasgow

How to Read this Work

Advocates of Abstract Algebra can omit Appendix A and Appendix C, and will be able to understand the work through brief perusal of the tables, and algebraic and numerical examples, during a search for the work contributions. Subsequently, the work should be read, where necessary, throughout

Other readers can omit Appendix A and Appendix C entirely upon a first reading. The flavour of the work will be delivered via a thorough initial perusal of the numerical tables, numerical examples, and diagrams. Following this, the work should be read throughout, without Appendix A, and Appendix C, then speed-read, with the inclusion of Appendix A and Appendix C, where possible.

References

[1]. *Elementary Number Theory*, Revised printing, **1988**, D.M. Burton.

[2]. *Advanced Engineering Mathematics*, 5th Edition, **2011**, K.A. Stroud.

Excluding new material, all terms used in this work can be found in the following two books:

Oxford Concise Dictionary of Mathematics, 4th Edition, **2009**, C. Clapham, J. Nicholson.

Collins Dictionary of Mathematics, 2nd Edition, **2002**, E.J. Borowski, J. M. Borwein.

Table of Contents

		Page
Section 1	Common Factor Pairs and Relatively Prime Pairs	1~10
Section 2	The Pattern in the Primes	11~16
Section 3	Counting Primes	17~20
Section 4	The Goldbach-Lee Theorem	21~22
Section 5	The Twin Prime Theorem	23~31
Section 6	Computing Primes	32~39
Section 7	Matrices and the Prime Matrix	40~45
Section 8	Quantum Space	46~50
Section 9	The Fermat-Lee Theorem	51~53

Appendix

		Page
Section A	Rings, Fields, Ideals, and Modules	1~11
	(requires an undergraduate course in Abstract Algebra and Group Theory)	
Section B	Module Mirror Primes (MMPs)	12~17
Section C	MMP Structure	18~23
Section D	Prime Modules of Modules of 30 Units	24~25

Contributions

Section 1	Mirror Factors, Mirror Relative Primes, The Prime Factor-pair Theorem.
Section 2	Module Mirror Factors, Modules of 30 Units, The Lee-Prime Theorem.
Section 3	Sieved Modules, Unsieved Modules, Prime Number Counting Algorithm.
Section 4	A Solution to the Goldbach Conjecture.
Section 5	A Solution to the Twin Prime Theorem, Twin Prime Indicators, Modules of Modules.
Section 6	Selection of Methods, Prime Computation Summation Algorithm, Lees Prime Summation Theorem, Lees Prime Summation Test.
Section 7	Antitrace, Eigenvalue Residue per Unit Distortion, Directions for Analysis.
Section 8	Lee's Equation, Principal Quantum Number Derivation, Pythagorean Triangles and Factor Sets, Atomic Theory Magic Number Set Generation.
Section 9	The Fermat-Lee Theorem:- the 'Wonderful' Proof Mentioned by Fermat ?

r	0	1	2	3	$\cdots$
λ_{1_i}	19	20	21	22	$\cdots$
λ_{2_i}	18	17	16	15	$\cdots$

$(*)+1$ $\underset{\rightarrow\infty}{}$; $(*)-1$ $\underset{\rightarrow -\infty}{}$

$$\Rightarrow x = 20 \bmod 3 \Rightarrow x = 2+3a$$
$$\Rightarrow x = 21 \bmod 5 \Rightarrow x = 1+5b$$
$$\Rightarrow x = 22 \bmod 7 \Rightarrow x = 1+7c$$

And $2+3a = 1 \bmod 5 \Rightarrow 3a = 4 \bmod 5 \Rightarrow a = 3 \bmod 5 \Rightarrow a = 3+5b$, so that $2+3a \Rightarrow 11+15b = 1 \bmod 7 \Rightarrow 3b = 5 \bmod 7 \Rightarrow b = 4 \bmod 7 \Rightarrow b = 4+7c$.

Thus $\Rightarrow$ $x = 11+60+105c = 71+105c$. And since $37 < 71$, we test $\gcd(37,71)$. As $\gcd(37,71) = 1$, then the value 37 is prime.

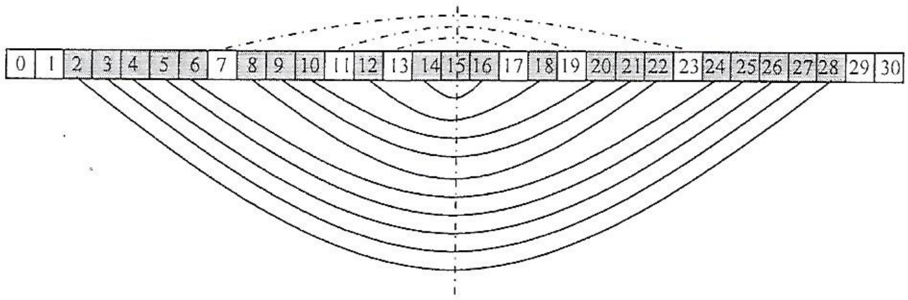
Section 2

The Pattern in the Primes

The construction of dual lanes of composite even, composite odd, and odd prime values, in the form of Folded Numbers (FNs) (Appendix B), demonstrates that where $p = \lambda_1 + \lambda_2$, $\lambda_1, \lambda_2 \in \mathbb{N}$, $\lambda_1, \lambda_2 \neq \{0,1\}$, and both λ_1 and λ_2 possess a common factor ≥ 1, (which subsequently is also a factor of $2i$ for p even, and $2i+1$ for p odd, where i indexes each of the λ_{1_i} and λ_{2_i}), then the pair of values λ_{1_i} and λ_{2_i} can be found in the same column, $r = i$. This means that the values containing a common factor $q = \gcd(p, \lambda_{1_i}, \lambda_{2_i})$, $i \in \{0,1,2,\ldots,r\}$, are the same distances from the start-point column indexed by $r = 0$. When $\lambda_1 = \lambda_2$, then the pairs of column-related factors are equal distances from the same point. An example of this relationship is detailed below, for the case $P = \lambda_1 + \lambda_2 = 30$, with $\lambda_1, \lambda_2 \in \{0,1\}$ necessarily excluded.

$r =$ 0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\lambda_{1_r} = 15$	16	17	18	19	20	21	22	23	24	25	26	27	28	~~29~~	~~30~~
$\lambda_{2_r} = 15$	14	13	12	11	10	9	8	7	6	5	4	3	2	~~1~~	~~0~~

Common-factor-less column pairs are relatively prime, and may also contain one, or two, primes. In the table above, common even factors in columns are related by a light-grey shaded long rectangle formed from two component rectangles below the emboldened line, whilst common odd factors in columns are related by a dark-grey shaded small single component rectangle above the emboldened line. The relationship is equivalent to the number-line $0 \sim 30$ shown below, in which the pairs of (shaded) factor-related values and pairs of (unshaded) primes $(7,23)$, $(11,19)$, $(13,17)$, are related through their summation to 30.



The factor products q in a FN, located in the same column as another factor product of the form $2n - q$, $n \in \mathbb{N}$, possessing the same factor, are termed as Mirror Factors (MFs) (Section

1, page 4). Where the mirror components of a FN are not MFs, then they are relatively prime (RP). Where both components are prime, we term them as Mirror Primes (MPs) (Appendix B). If a module (Appendix A, page 10) of the form $n=\prod_{i=1}^{r} p_i : i=\{1,2,\ldots,r\} \quad p_i \in \mathbb{P}, \quad p_1=2,$ $p_2=3, \quad p_3=5,\ldots,$ (Appendix C), with n necessarily even, describes the mirror factor $\left(q, \prod_{i=1}^{r} p_i - q\right),$ $r=\mathbb{Z}^+$, $q \in \mathbb{N}$, then we term the module, a MF module (MFM), and the Relatively Prime (RP) components as MRPs. When two primes can be related in the same way, we term the pair, Module Mirror Primes (MMPs), expanded upon in Appendix B. MFMs of (necessarily) even length $\mathbb{Z}_n$, $n=\prod_{i=1}^{r} p_i$, $n \in 2\mathbb{N}_{>1}$, satisfy modular arithmetic modulo n, in which $\mathbb{Z}_n$, is a ring $(\mathrm{MP}(n),*)$, (Appendix A, page 6) as well as a module. The module $\mathbb{Z}_n$, $n=\prod_{i=1}^{3} p_i = 30$, denoted $\mathbb{Z}_{30}$, is a module over the ring $\mathbb{Z}$, generating $\mathbb{Z}$, partitioned at each $30n, \ n=\mathbb{N}$.

Considering now, modules formed as the canonical prime-products

$$\prod_{i=1}^{1} p_i := p_1 = 2, \quad \prod_{i=1}^{2} p_i := p_1.p_2 = 2.3 = 6, \quad \prod_{i=1}^{3} p_i := p_1.p_2.p_2 = 2.3.5 = 30,$$

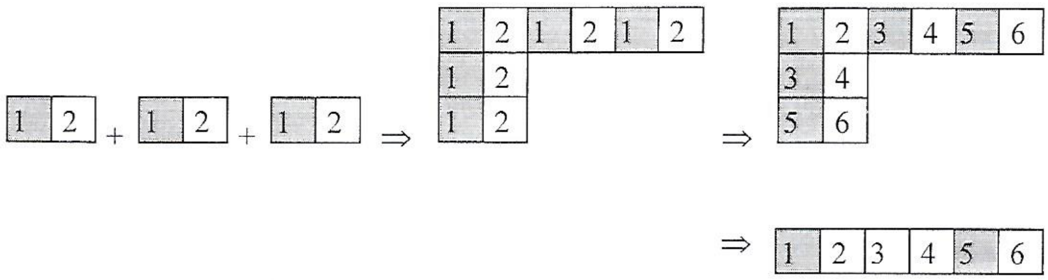
and in general,

$$\prod_{i=1}^{r} p_i = p_1.p_2.\ldots.p_r,$$

then, by construction, all prime-products generated are even, since $p_1 = 2$, and they then operate as prime-product $R-$modules (PPRMs). All PPRMs are MFMs.

Returning to modules over the ring of integers $\mathbb{Z}$, we begin with the module of length $\prod_i p_i : i=1 \Rightarrow p_1 : p_1 = 2$ units. A visual representation of this $\mathbb{Z}_2$ module is, | 1 | 2 |, where we can note that whilst 2 is the only even prime, so that $\forall n \in \mathbb{N},\ 2n$ is composite, the shaded area has as a subset, the set of odd numbers, of which a subset is the set of odd primes. That is, every odd prime is of the form $2n+1, n \in \mathbb{N}$. Thus a row of arbitrary length $n \in \mathbb{N}$, represented as $\mathbb{Z}_2$ modules, will always have the odd numbers n, congruent to $\mathbb{Z}_2$ modulo 1, and the even numbers n, congruent to $\mathbb{Z}_2$ modulo 2.

Moving now to the module of length $\prod_i p_i : i = \{1,2\} \Rightarrow p_1.p_2 \Rightarrow 2.3 = 6$ units, and forming the module of 6 units via concatenation of three two-unit modules $\Rightarrow 2+2+2=6$. We can represent this $\mathbb{Z}_6$ module visually, as the sum of three $\mathbb{Z}_2$ modules, with the new prime 3, and its multiples, excluded:



We can then note that since $2, 4$, and 6 are even, and 3 (and 6) are divisible by the new prime 3, then concatenation of the modified $\mathbb{Z}_6$ modules

1	2	3	4	5	6	1	2	3	4	5	6	1	2	3	4	5	6

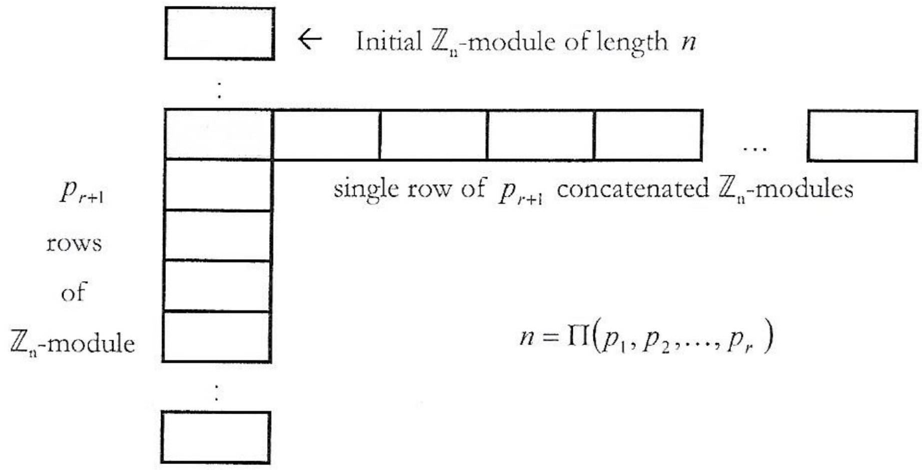
...

provides a visual representation of the corresponding fact that all odd primes > 3, are of the form $6k \pm 1,\ k \in \mathbb{N}$. [1]. In any concatenation of any length, of $\mathbb{Z}_6$ modules, since we have excluded only the primes 2 and 3, and their multiples, then no value (greater than 1) remaining in the concatenation equivalent in $\mathbb{N}$, will contain a multiple of 2 or 3. Here, using three $\mathbb{Z}_6$ modules, this is

·	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18

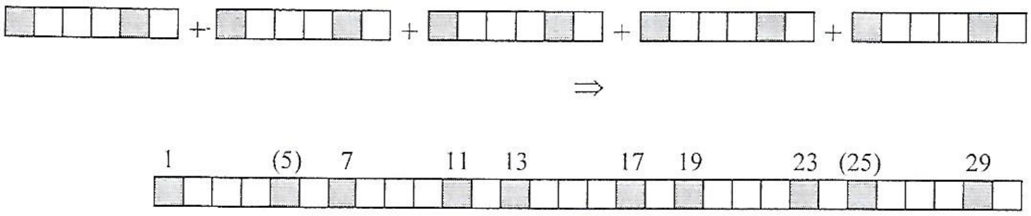
which delivers the (shaded) values 5, 7, 11, 13, 17, ..., all of which are prime. Note that following this methodology, the first shaded composite would be the square of 5, $5*5 = 25$, and the next would be 35, which expressed as a product of primes, is $35 = 5*7$.

In general, when the MFMs are $R-$modules of the form $\mathbb{Z}_n$-modules, $n = \prod_{i=1}^{r} p_i$, then $n \in 2\mathbb{N}$, and $\mathbb{Z}_n$ is a module over the ring $\mathbb{Z}$, (Appendix A), and the values $\mathbb{Z} \leq n = \prod_{i=1}^{r+1} p_i$, can be represented as p_{r+1} stacked rows of the initial $\mathbb{Z}_n$-module, or as a single length of p_{r+1}, $\mathbb{Z}_n$-modules in series, as indicated below.

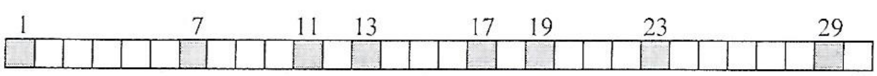


In order to generate the next initial $\mathbb{Z}_n$-module, we must remove the latest (new) prime, and its multiples. The module-generation procedure is then iterated. In these representations, the properties of FNs, MMFs and MMPs, are always valid.

We can thus consider the next module in the sequence, of length $\prod_i p_i : i = \{1,2,3\} \Rightarrow p_1.p_2.p_3 \Rightarrow 2.3.5 = 30$ units, formed via concatenation of five, 6-unit modules $\Rightarrow$ $6+6+6+6+6 = 5*6 = 30$. The $\mathbb{Z}_{30}$ module can be represented visually, following the same methodology detailed above, (but excluding generation of the five stacked rows, for clarity), whose structure is detailed in Appendix C, as



which, with the latest (new) prime 5, and its multiples removed from the module $\Rightarrow$



Note that in this work, the value 1, in an n^{th} module in a concatenation of modules, is interpreted as a value 31, in the $(n-1)^{\text{th}}$ module. This will be indicated as (3)1. Thus the modules of 30 elements are partitioned as $\{(3)1, 2, 3, \ldots, 29, 30\}$. Each $\mathbb{Z}_{30}$ module can describe a maximum of eight primes $30m + \{(3)1, 7, 11, 13, 17, 19, 23, 29\}$, $m \in \mathbb{N}^0$, with each module (excluding the first, since 1 is not a prime) implying three twin primes $\{(11,13), (17,19), (29,(3)1)\}$, and the related twin primes $\{30u + (11,13),\ 30v + (17,19),\ 30w + (29,(3)1)\}$, for various $u, v, w \in \mathbb{N}^0$.

Since the primes used to construct the $\mathbb{Z}_{30}$ module, and their multiples, corresponding to the clear squares, are removed from the module and partition the module, then excluding the value 1, every other value in the module will correspond to a prime, or a product of primes, each prime component of which is greater than the largest prime used to construct the module. Through concatenation of processed $\mathbb{Z}_n$-modules in this iterative manner, a recurring pattern of composite (stacked row) lanes, generated by the primes less than or equal to p_r, and their respective composites, generates the pattern in the primes. Note that generation of a $\mathbb{Z}_n$-module $n = \prod_{i=1}^{r} p_i$, only ensures that the values $\{1, 2, \ldots, p_{i+1}^2 - 1\}$ have been properly sieved for primes. Thus the pattern is described via the regularity of generation, and the symmetry involved, outside of the properly primed values $\{1, 2, \ldots, p_{i+1}^2 - 1\}$, in the region $\left[1, 2, \ldots, p_{i+1}^2, \ldots, \prod_{i=1}^{r+1} p_i\right]$, through the generation of sequential prime modules, prior to removal of the latest (new) prime, and its multiples from the newly generated module, examples of which are presented in Appendix B, with module structure clarified in Appendix C.

We can be further assured that the pattern is the general pattern sought, since the removal, from any initial module, of primes less than or equal to p_r, and the subsequent concatenation of the processed module, generates the recurring omission of primes in any new, larger module, for every value of p_r, $r = \mathbb{N}$, at both ends of each concatenated module. Examples of this patterning for the values 30, 210, and 2310, are demonstrated in Appendix B. We can note at this point, that where the Goldbach Conjecture, that every even number > 2 is a sum of two primes, is proven to be true, then every MFM contains a MMP pair.

Considering the row of values of a FN containing the smaller values $\left[1, \frac{1}{2}\prod_{i=1}^{r} p_i\right]$, and the row of larger values above them, $\left[1+\frac{1}{2}\prod_{i=1}^{r} p_i, \prod_{i=1}^{r} p_i\right]$ then the properties of FNs, MFMs, and MMPs give rise to the following general theorem:

The Lee-Prime Theorem

Given an odd integer

$$m \in \left]p_r, \frac{1}{2}\prod_{i=1}^{r} p_i\right[, \quad p_i \nmid m, \ p_r \in \mathbb{P}, \ r = \mathbb{N}_{>1}, \quad p_1 = 2, \ p_2 = 3, \ p_3 = 5, \ldots,$$

then

$$\Psi = \begin{cases} \prod_{i=1}^{r} p_i - m, & m \text{ an odd prime} \\ \prod_{i=1}^{r} p_i - m, & m \text{ composite (including prime to a power)} \end{cases},$$

is a prime $\Psi = p_{q_1} > p_r$,

is a power $n \in \mathbb{N}_{>1}$ of a prime $p_{q_1} > p_r$: $\Psi = p_{q_1}^{n}$,

or is a composite formed from primes $p_{q_{\|j\|}}$, $j > 1$: each $p_{q_{\|j\|}} > p_r$, and $\|j\|$ counts the distinct primes : $\Psi = \prod_j p_{q_j}^{n_j}$, for some values of $p_{q_j} \in \mathbb{P}$, $n_j \in \mathbb{N}$.

Let a prime of the form Ψ be termed

Lee-prime if m is prime,

and

Lee-composite-prime if m is composite.

Subsequently, every prime is either Lee-prime, or Lee-composite-prime. The primality of Ψ can be determined trivially, through (Zeusian) examination of $\gcd(\Omega, \Psi)$, where

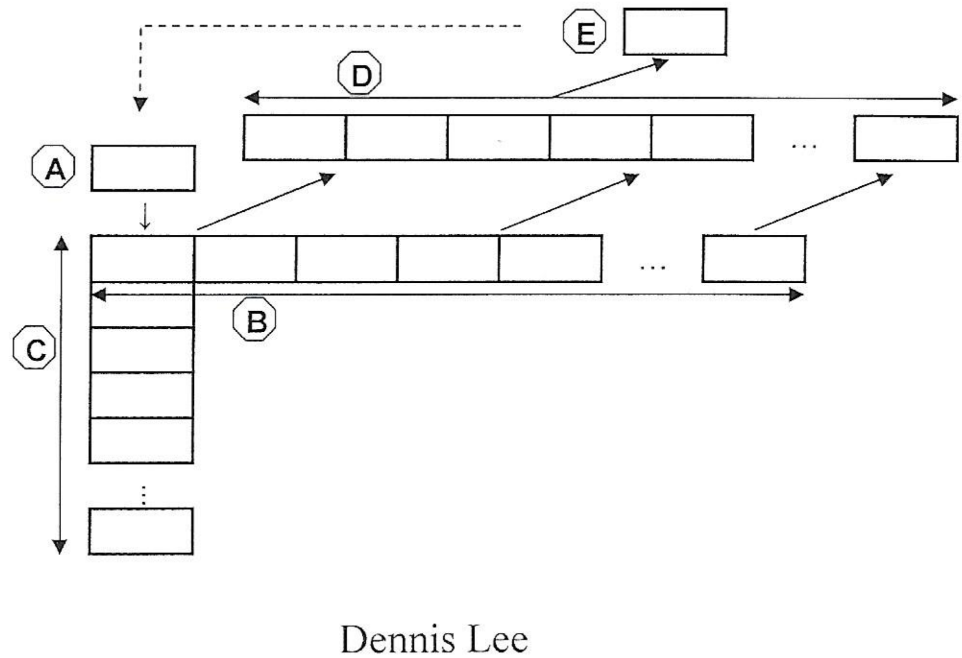
$\Omega = \prod_{k=1}^{w} p_k$: $p_w \leq \left[\sqrt{\Psi}\right]^g < p_{w+1}$, for $[*]^g$ the greatest integer function.

Section 3

Counting Primes

It has been demonstrated in Section 2, page 14, that given an initial $\mathbb{Z}_n$-module of length n, labeled 'A' in the diagram below, for which $n = \prod_{i=1}^{r} p_i$, then since $p_{r+1}.n = p_{r+1} \prod_{i=1}^{r} p_i = \prod_{i=1}^{r+1} p_i$, we can form the next module, the $\mathbb{Z}_{n+1}$-module, via concatenation as a single row of p_{r+1} $\mathbb{Z}_n$-modules, labeled below as B, or equivalently, as a set of p_{r+1} aligned rows of the $\mathbb{Z}_n$-module, labeled as C. Every sub-module of the concatenation of modules described in A, B, and C, possesses precisely the same structure; thus removing in both B, and C, the multiples of each of the primes used in order to form the initial $\mathbb{Z}_n$-module, labeled as A. Suppose now, that initial module A is subsequently 'sieved' in order to ensure that the module contains only primes. We shall term such a module as a sieved module (SM). Correspondingly, excluding the initial sieved module (SM) A, we shall term all other sub-modules of B, and C, (which necessarily contain composites), as unsieved modules (uSM).

We are now in a position to remove all of the composite values from B (and equivalently C), via the removal of any primes $\leq \left[\sqrt{\prod_{i=1}^{r+1} p_i} \right]^g$, which were not removed earlier, and their multiples, where $[*]^g$ denotes the greatest lower bound. We shall denote the largest prime $\leq [*]^g$, as $[*]^{gp}$, implying $p_j = \left[\sqrt{\prod_{i=1}^{r+1} p_i} \right]^{gp}$, wrt an initial module of length $n = \prod_{i=1}^{r} p_i$.



Removing the additional primes and their multiples from module B (and/or equivalently module C), generates the sieved module (SM) of modules, indicated above as D. The SM of modules D, is entirely equivalent to the single module E, of length $m = \prod_{i=1}^{r+1} p_i$.

Thus, the work here, in conjunction with the details provided in Section 1, Section 2, and the Appendices Section A, Section B, and Section C, inform us that there are three different types of prime module; those we have met earlier, which have the canonically listed primes in ascending order and their multiples, removed; those which have had values removed as the primes used in order to generate a new (sieved) module and their multiples, termed SMs; and the untreated list of modules of identical structure termed uSMs.

Since the structure of each of the sub-modules of the uSMs B, and C, is precisely the same, then excluding row one, any primes evident in any row, will be located in the same column positions as those primes (and/or squares), in row 1. Also, since the concatenation of the sub-modules of the uSMs B, (and equivalently C), delivers an even value, which is then symmetric about a central value, then where we treat the uSM as a FN, Bertrands Postulate proven by Chebyshev, that for any integer $n > 3$, there is always at least one prime p_j between n and $2n-2$ [1], implies that the list of upper numerically greater values of the corresponding SM FN will always contain at least one prime. Since we are dealing with a SM, then by the property of MMPs (Appendix B), any upper-value SM FN prime will always sit above either a prime, or a square, and be larger than the largest prime component used to generate the SM, or a prime raised to a power, whose prime component is larger than the largest prime component used to generate the SM.

Delivering an approximate count of the number of primes and/or twin primes less than or equal to any value $n \in \mathbb{N}$, is assisted through initial use of the module of length $n = \prod_{i=1}^{3} p_i = 30$, described in Section 2, page 14, shown below, as a measure,

(3)1						7				11		13				17		19				23						29	

in which as earlier, the value (3)1 at position 1, implies the prime value 31. This possesses 3 twin primes $\{(11,13),(17,19),(29,(3)1)\}$, and two single primes $\{7,23\}$, or alternatively, 8 single primes in total. We shall label the total number of primes generated at any stage r, by ξ_r.

The basis for a third-stage calculation is then $\xi_3 = 8$, and ξ_r then needs to be determined for each stage $n \in \mathbb{N}_{>3}$. The iterative procedure for the generation of new primes in addition to those already secured in a module, is that the r^{th} module space is concatenated (in a single line, or as a list of module rows) p_{r+1} times, whereupon all of the composites are removed, thus leaving a list of primes, some of which were earlier generated, and others which are new primes. This implies the iterative function $\xi_r = p_r \xi_{r-1} - \eta(r)$, in which $\eta(r)$ counts the number of removed, newly generated composite values. An efficient algorithm generating $\eta(n)$, for any $n \in \mathbb{N}$, for which $\eta(r)$ is a subset, follows:

Secure the list of prime numbers less than or equal to $\left[\sqrt{n}\right]^{gp} \in \mathbb{N}$, (in this work, we are dealing specifically with the case $n = \prod_{i=1}^{r} p_i$).

STEP 1: Beginning with the smallest prime number, $p_1 = 2$, form the list of composites containing the value 2, in canonical sequence, from 2, to $\left[\frac{n}{2}\right]^g$, where $[*]^g$ denotes the greatest lower bound. This is simply the set of values $2.\{1, 2, \ldots, \frac{n}{2}\}$.

STEP 2: Moving to the next largest prime, $p_2 = 3$, form the list of composites containing the value 3, in canonical sequence, from 3, to $\left[\frac{n}{3}\right]^g$, excluding any values in the list which contain any prime smaller than the current prime. This is the prime $p_2 = 3$, followed by the square 3^2, then the ascending list of primes, and composites formed from primes greater than $p_2 = 3$, taken from the set of values $\{(3^2+1), \ldots, \frac{n}{2}\}$.

STEP 3: Dealing now with each prime p_i in sequence, we follow the methodology delineated in STEP 2, until the list of primes and composites $\leq \left[\sqrt{n}\right]^g \in \mathbb{N}$, is depleted.

STEP 4: Sum each final number of components generated, remove the initial number of generating primes, and add 1, for the listed value 1. The total is the total number of composite values in the list $\{2, \ldots, n\}$, plus 1, which we have earlier denoted as $\eta(r)$. The number of primes in the list $\{1, 2, \ldots, n\}$, is then $n - \eta(r)$.

An example, for the case $n = \prod_{i=1}^{3} p_i = 30$, follows:

$\left[\sqrt{30}\right]^g = 5, \Rightarrow$ the set of primes $\{2, 3, 5\}$, so that

$$2 \Rightarrow \left[\frac{30}{2}\right]^g = 15, \quad \Rightarrow \quad \{2, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11, 2.12, 2.13, 2.14, 2.15\},$$

$\Rightarrow 2 \Rightarrow \{2,4,6,8,10,12,14,16,18,20,22,24,26,28,30\}$, with 15 components.

$3 \Rightarrow \left[\frac{30}{3}\right]^{g} = 10, \;\Rightarrow\; \{3, 3.3, 3.5, 3.7, 3.9\}$,

$\Rightarrow 3 \Rightarrow \{3,9,15,21,27\}$, with 5 components.

$5 \Rightarrow \left[\frac{30}{5}\right]^{g} = 6, \;\Rightarrow\; \{5, 5.5\}$,

$\Rightarrow 5 \Rightarrow \{5,25\}$, with 2 components.

The total number of composites (plus 1), is then given by $\eta(r) = 15+5+2 = 22$, minus the three generating primes $\Rightarrow\; 22-3=19$, and plus 1, for the listed value 1, $\Rightarrow\; 19+1=20$. And since $30-20=10$, $\Rightarrow$ the set of ten prime values ≤ 30 is, $\{2,3,5,7,11,13,17,19,23,29\}$. For (subsequently) larger values, calculation of the prime-product lists wrt each prime p_i, can begin with the maximum value of the lists earlier generated.

Section 4

The Goldbach-Lee Theorem

Theorem

For all $n : n \in \mathbb{N}_{>1}$, the list of $p_i + q_i = 2n$, $p_i, q_i \in \mathbb{N}$, $i \in \mathbb{N}$, always contains at least one prime pair, $p_k, q_k \in \mathbb{P}$, such that $p_k + q_k = 2n$, $k \geq 1$, every even number ≥ 4 can be written as the sum of two primes, and every even number ≥ 6, can be written as the sum of two odd primes.

The proof is demonstrated by construction of the list of prime values $< 2n$ and the list of each respective residue summing to $2n$, followed by assumption of a hypothesis, and subsequent contradiction.

Consider an arbitrary value $2n$, $n \in \mathbb{N}_{>2}$, and the set of primes $\mathbb{P}$ in canonical ascendance, $p_i \in \mathbb{P}$, $p_1 = 2$, $p_2 = 3$, $p_3 = 5, \ldots,$ $2 \leq p_i < 2n$,

then $\exists$ values $q_i \in \mathbb{N}_{>3}$, $\forall i$:

$$1 \leq i \leq r < 2n,\ 3 < q_i < 2n : \ r \text{ counts the pair sums, and } p_i + q_i = 2n,\ n \in \mathbb{N}_{>3}.$$

The possible values of the related pairs p_i and q_i, are displayed in the Table below, in general form. The (even) pair (p_1, q_1), is included in the Table, for clarity.

Index Values r	List of Primes p_i	Prime/Composite q_i
1	$p_1 = 2$	$q_1 = 2n - 2$ $(q_1\ even)$
2	$p_2 = 3$	$q_2 = 2n - 3$
3	$p_3 = 5$	$q_3 = 2n - 5$
$\vdots$	$\vdots$	$\vdots$
i	$p_i = 2n - q_i$	$q_i = 2n - p_i$
$\vdots$	$\vdots$	$\vdots$
$r-1$	$p_{r-1} = 2n - q_{r-1}$	$q_{r-1} = 2n - p_{r-1}$
r	$p_r = 2n - q_r$	$q_r = 2n - p_r$

The values in list $q_i \in \mathbb{N}_{>2}$, can be of any of three forms:

i. All primes
ii. Mixture of primes and composites
iii. All composites

We shall proceed via assuming that the list does not contain a prime, and seek a contradiction, whence the list must contain at least one prime q_k say, thereby forming at least one pair of primes (p_k, q_k): $p_k, q_k \in \mathbb{P}$, $p_k + q_k = 2n$, or one coinciding prime $p_k = q_k$.

If the list of values q_i does not contain a prime, then the list must all be composite. Since they are all composite and $< 2n$, then by the definition and properties of primality, each of them is divisible by at least one of the primes $p_{k_1}, p_{k_2}, \ldots, p_{k_m}$, in ascendance, the series of primes that divide $2n$, $p_{k_i} \in \mathbb{P}$, such that $p_{k_i} \mid 2n$ and $p_{k_i} < \left[\sqrt{2n}\right]^g$.

Consider now, any prime $p_h : p_{k_m} < p_h < 2n$, so that in particular, $p_h \neq p_{k_i}$, $\forall i \in \{1, 2, \ldots, m\}$. We know $\exists$ at least one such p_h : $n < p_h < 2n$, by Bertrands Postulate proven by Chebyshev, that for any integer $n > 3$, there is always at least one prime p_j between n and $2n-2$ [1]. Equivalently, noting that for $n \geq 8$, we always have $\frac{n}{2} > \sqrt{2n} > \left[\sqrt{2n}\right]^g$, then the corresponding bound can be written as p_h : $\frac{n}{2} < p_h < n$.

The respective related composite of the prime p_h, is given as $q_h = 2n - p_h$.

But since q_h is composite and $< 2n$, then at least one of the primes $p_{k_1}, p_{k_2}, \ldots, p_{k_m}$, dividing $2n$, must also divide q_h. We shall label a prime dividing q_h, as p_{k_i}, so that we must always have

$$p_{k_i} \mid 2n \quad \text{and} \quad p_{k_i} \mid (q_h = 2n - p_h).$$

But then the statements imply that $p_{k_i} \mid p_h$, which, by the definition of primality, is true if and only if $p_{k_i} = p_h$. However, $p_{k_i} = p_h$ contradicts the statement $p_h > p_{k_m} \geq p_{k_i}$. Noting also that if p_h is composite, then this contradicts the primality of the Bertrands Postulate -derived prime p_h.

Hence the (dual) contradiction indicates that our original assumption is in error, and thus, not all of the q_i are composite.

Hence at least one of the list of divisors q_k, must be prime, and thus for all $n : n \in \mathbb{N}_{>3}$, the list of $p_k + q_k = 2n$, $n \in \mathbb{N}_{>3}$ always contains at least one prime pair, $p_k, q_k \in \mathbb{P}$: $p_k + q_k = 2n$. Noting also that $2+2=4$, and $3+3=6$, then every even number ≥ 4, can be written as the sum of two primes, and every even number ≥ 6, can be written as the sum of two odd primes.

Section 5

The Twin Prime Theorem

Theorem

There exist an infinite number of pairs of successive odd integers p and $p+2$, $p,(p+2)\in\mathbb{Z}$, such that $p,(p+2)\in\mathbb{P}$, the set of primes in canonical ascendance.

The proof is demonstrated by construction of Noetherian modules, (Appendix A, page 10), followed by assumption of a finite number of twin primes, and contradiction.

Proof methodology is similar to the generation of primes by way of the Sieve of Eratosthenes. The methodology developed by Eratosthenes of Cyrene (276~194 BC), a Greek mathematician, consists of writing-down the positive integers, from 2, to some (finite) value n, in their natural ascending order, and then systematically removing all the multiples (thus composites) of the primes $p\leq\sqrt{n}$ [1]. Those integers remaining in the list are determined to have been 'sieved', and are subsequently primes.

Given that the square root of 100, equals 10, an Eratosthenian sieve of the first 100 positive integers is shown below, in which each prime has been emboldened, and composites ≤ 100, have been marked in the following manner:

Divisible by: $2\Rightarrow$ (removed) $3\Rightarrow$ —, $5\Rightarrow$ |, $7\Rightarrow$ /.

	2	3		5		7		~~9~~	
11		**13**		~~15~~		**17**		**19**	
~~21~~		**23**		~~25~~		~~27~~		**29**	
31		~~33~~		~~35~~		**37**		~~39~~	
41		**43**		~~45~~		**47**		~~49~~	
~~51~~		**53**		~~55~~		~~57~~		**59**	
61		~~63~~		~~65~~		**67**		~~69~~	
71		**73**		~~75~~		~~77~~		**79**	
~~81~~		**83**		~~85~~		~~87~~		**89**	
~~91~~		~~93~~		~~95~~		**97**		~~99~~	

Thus the values 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, and 97, are the primes ≤ 100. In particular, the list of twin primes ≤ 100 can then be seen to be

$$(3,5),(5,7),(11,13),(17,19),(29,31),(41,43),(59,61),(71,73).$$

We now consider, the module of 30 units, denoted module_{30}, or more concisely, M_{30}, formed in Section 2, page 14, and shown below, which we use as a measure.

1						7				11		13				17		19				23						29	

The M_{30} describes 8 primes, $\{7,11,13,17,19,23,29,(3)1\}$, of which three pairs, $\{(11,13),(17,19),(29,(3)1)\}$, are twin primes. It is partitioned by the (prime) values 2, 3, and 5, and their multiples ≤ 30. The value $(3)1$ is also indicated by a shaded square, in the position of 1 unit.

Concatenation of n of the M_{30}, implies that any value $q \in \mathbb{N}$, can be formed from a multiple of r of the M_{30}, plus a residue $s : 0 \leq s < 30,\ s \in \mathbb{N}^0$. That is, the division algorithm $q = 30r + s$, for any value q (Appendix A, page 2) [1]. Thus the value q can be addressed by r of the M_{30}, plus a non-negative integer residue < 30, contained in the M_{30}, in the manner of the Table shown below.

$\mathbb{Z}^+ \downarrow$					Modules of 30 units $\downarrow$
1	$\Rightarrow$	1	$\rightarrow$	30	
2	$\Rightarrow$	31	$\rightarrow$	60	
3	$\Rightarrow$	61	$\rightarrow$	90	
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	
r	$\Rightarrow$	$(r-1).30+1$	$\rightarrow$	$r.30$	
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	

The values in this Table correspond to the values in Appendix D, Table, column (a), and column (b). That is, any value $x : x \in [(r-1).30+1, r.30]$ can be found in the r^{th} row of the M_{30}, $r = \mathbb{N}$. In particular, this means that, any $\mathbb{Z}^+$-addressed M_{30}, in the manner of that shown in the Table above, contains a maximum of two pairs of twin primes in the columns beneath the values $(11,13)$, and $(17,19)$, plus a third twin prime in the columns beneath $(29,(3)1)$, which includes the first element (in the column corresponding to the value 1) of the following row.

We can then attach to each module row (and first component of the next row), an indication as to the presence of the potential twin primes, $30k + \{(11,13),(17,19),(29,(3)1)\}$,

$k \in \mathbb{Z}^+$. We do this through construction of the Twin Prime Indicator mod_{30} (TPI_{30}), $(*,*,*)$, for $* \in \{0,1\}$, or equivalently, └┴┘, for visual clarity, in which each vertical strut is either present, or omitted. The leftmost indicator implies the values $(11 \text{ and/or } 13)$, the centre indicator implies the values $(17 \text{ and/or } 19)$, and the rightmost indicator implies the values $(29 \text{ and/or } (3)1)$, and we respect the position of the value $(3)1$, and its corresponding indicator.

Thus we have the TPI_{30} of form $(1,1,1)$, or └┴┘.

When any one of the values in $\{(11,13),(17,19),(29,(3)1)\}$, is removed, thus removing any possibility of presence of a corresponding TP, the TPI_{30} is modified as being removed. Thus we have the eight TPIs_{30} detailed below in both numerical form, and as a visual aid. In this work, in order to furnish expediency of communication, we will be relying upon the visual form:

$(1,1,1)$	└┴┘	All TPIs_{30} present (shortened in this work to —)
$(0,1,1)$	─┴┘	TPIs_{30} $(11 \text{ and/or } 13)$ removed
$(1,0,1)$	└─┘	TPIs_{30} $(17 \text{ and/or } 19)$ removed
$(0,0,1)$	──┘	TPIs_{30} $(11 \text{ and/or } 13)$, and $(17 \text{ and/or } 19)$, removed
$(1,1,0)$	└┴─	TPIs_{30} $(29 \text{ and/or } (3)1)$ removed
$(0,1,0)$	─┴─	TPIs_{30} $(11 \text{ and/or } 13)$, and $(29 \text{ and/or } (3)1)$ removed
$(1,0,0)$	└──	TPIs_{30} $(17 \text{ and/or } 19)$, and $(29 \text{ and/or } (3)1)$ removed
$(0,0,0)$	⨯	Omitted TPIs_{30} $(11 \text{ and/or } 13)$, $(17 \text{ and/or } 19)$, and $(29 \text{ and/or } (3)1)$

Or more concisely,

{ — ─┴┘ └─┘ ──┘ └┴─ ─┴─ └── ⨯ } corresponding to

$\{(1,1,1), (0,1,1), (1,0,1), (0,0,1), (1,1,0), (0,1,0), (1,0,0), (0,0,0)\}$

The operation of intersection $(\cap)$ on TPIs_{30} follows precisely, the Boolean operation of 'logical and', $(\wedge)$, so that for instance,

$(1,1,1)\cap(1,0,1)\Leftrightarrow(1,1,1)\wedge(1,0,1)=(1,0,1)$ or — ∩ ⊔ = ⊔

$(0,1,1)\cap(0,1,0)\Leftrightarrow(0,1,1)\wedge(0,1,0)=(0,1,0)$ or ┴┘ ∩ ⊥ = ⊥

$(0,1,0)\cap(1,0,0)\Leftrightarrow(0,1,0)\wedge(1,0,0)=(0,0,0)$ or ⊥ ∩ └ = ×

We now form a module of the M_{30}. Consider each prime module, M_{p_i}, of M_{30}, denoted $M_{p_i\times 30}$, comprising p_i rows of M_{30}, $p_i \in \mathbb{P}_{>5}$, in which the first (prime) value in each $M_{p_i\times 30}$, is the value p_i in the upper bounded rectangles shown in Appendix D, Table, (d), (g), (i), (j), (k), (l), (m), (n).

Congruence modulo n is an equivalence relation, and so defines a partition of the set of integers, where two integers are in the same class iff they are congruent modulo n. The classes are residues or congruence classes modulo n. Two integers are in the same class if they have the same remainder upon division by n. The residue classes are usually $\{[0],[1],[2],\ldots,n-1\}$ [1]. In this work, the field of operation is $\{[2],[3],\ldots,[30],[(3)1]\}$. Thus, since $\gcd(p_i,30)=1,\ i>3$, then the multiples of p_i in $M_{p_i\times 30}$, are congruent to $(n.p_i)\bmod 30$, which is thus soluble (Appendix A, page 4), and the 30 elements are partitioned as $n=\{(3)1,2,3,\ldots,29,30\}$.

For $p_4=7$, the $M_{p_4}=M_7$, of M_{30}, given as $M_{7\times 30}$, below, is seven rows of modules of 30 units, with first value 7, and subsequent multiples of 7, removed.

1	1	—	7	14	21	28		—
2	31	—	5	12	**19**	26		└┘
3	61	—	3	10	17	24		└─
4	91	—	31	8	15	22	29	└┴
5	121	—	6	13	20	27		─┴┘
6	151	—	4	11	18	25		─┴┘
7	181	—	2	9	16	23	30	—

Here, we display only those values which are removed $\bmod p_i$, as multiples of the prime p_i, and recall that we are examining the Twin Primes, which are shaded light grey. The positions of the two, possible primes, 7 and 23, which are not twin primes, are shaded dark grey. Also, the value congruent $\bmod 30$, to p_i^2, here $7^2=49$, is $19=49\bmod 30$, which is indicated by a small emboldened square.

Thus when a product of p_i in the modules_{30}, is equal $\bmod p_i$, to any of $\{11,13,17,19,29,(3)1\}$ we modify the corresponding TPI_{30}. Without modification, the $M_{7\times 30}$ is given by seven rows of the values $(3)1 \sim 30$ portrayed in line 24, and is indicated by the TPI_{30} —, in the third column of the Table above.

Now modifying the $\text{module}_{p4} = M_7$, through removal of the products of $p_4 = 7$, implies the TPI_{30} modifications shown in the final column of the Table above. Note that the value $(3)1$ in line 4, acts to modify the final TPI_{30} in the previous line, line 3, and not in its current line, line 4. Hence although the value 1 appears in row 4, the deletion corresponding to $(3)1 \equiv_{30} 1$ takes place in row 3.

We can then concatenate the set of seven rows, to form a list of as many rows as we like. Note that rows one and seven of the $M_{7\times 30}$ remain unmodified, whilst rows two to six, become modified.

Unmodified rows, indicated in column 3 of the Table above, in a list of $M_{7\times 30}$, then correspond to rows $\{1,7\}+7n$ for $n \in \mathbb{Z}_{30}$ at rows $\{1,7,8,14,15,\ldots,7n,7n+1,\ldots\}$, $n \in \mathbb{N}^0$. Since each $M_{7\times 30}$ in a list of n modules of modules_{30} possesses precisely the same TPI_{30} structure, then the removal or deletion of the multiples of $p_4 = 7$ implies a list of concatenated rows of seven TPIs_{30} corresponding to the (transpose) series

{ — └┘ └─ └┴─ ─┴┘ ─┴┘ — }, or its equivalent form,

$\{(1,1,1), (1,0,1), (1,0,0), (1,1,0), (0,1,1), (0,1,1), (1,1,1)\}$.

Using the same methodology, we can form $M_{p_i\times 30}$, for each $p_i \in \mathbb{P}$, $i \geq 4$ (since the smaller primes $2,3,5$, have already been used in the construction of the M_{30}). These $M_{p_i\times 30}$, correspond to the columns of $M_{p_i\times 30}$, shown in Appendix D, Table, (d), (g), (i), (j), (k), (l), (m), (n), for $p_i = 7,11,13,17,19,23,29,31$, respectively.

Each column list of $M_{p_i\times 30}$, for each $i \in \mathbb{Z}_{>3}$, corresponds to the removal of multiples of each $p_i \in \mathbb{P}$, $i \in \mathbb{Z}_{>3}$. Thus we now need to be in a position to remove the multiples of each prime, in succession, in their natural order. This will have the effect of removing all of the multiples of $p_4 = 7$, then the multiples of $p_5 = 11$, followed by the multiples of $p_6 = 13$, to use of any chosen value of $p_i \in \mathbb{P}$, $i \in \mathbb{Z}_{>3}$. This is in the same vein as the removal of multiples, in the methodology of the Sieve of Eratosthenes.

Following the removal of the multiples of any particular $p_i \in \mathbb{P}$, $i \in \mathbb{Z}_{>3}$, we then need to inspect the TPIs$_{30}$, in order to discover the effect on each row set of the three possible twin primes. We do this via use of the operation of intersection, which corresponds precisely with the Boolean operation of 'and' $(\wedge)$, wrt the modified state of TPIs$_{30}$ immediately preceeding any $M_{p_i \times 30}$, and the standard concatenated TPIs$_{30}$ of the $M_{p_i \times 30}$. Note that all M_{p_i}, excluding M_7, display their standard concatenated (so repeated) p_i-division-modified TPIs$_{30}$, to the left of the M_{p_i}, and the module-intersection modified TPIs$_{30}$, to the right of the modules$_{p_i}$. An example, beginning with an entirely unmodified list of TPIs$_{30}$, (A), and then removing multiples of $p_4 = 7$, (B), followed by removal of multiples of $p_5 = 11$, (C), is detailed below, in which the modified TPIs$_{30}$ of M_7, intersect with the standard TPIs$_{30}$ of M_{11}, via ((column B) $\cap$ (column C)) = column D. The concatenated forms can be viewed in Appendix D, Table.

		A						B	C				D
1	1	—	7	14	21	28		—	┴┘	11	22		┴┘
2	31	—	5	12	19	26		⊔	—	3	14	25	⊔
3	61	—	3	10	17	24		└	⊔	6	17	28	└
4	91	—	31	8	15	22	29	└┴	└┴	9	20		└┴
5	121	—	6	13	20	27		┴┘	—	31	12	23	┴┘
6	151	—	4	11	18	25		┴┘	—	4	15	26	┴┘
7	181	—	2	9	16	23	30	—	└┴	7	18	29	└┴
8	211	—						—	—	10	21		—
9	241	—						⊔	┴┘	2	13	24	┘
10	271	—						└	—	5	16	27	└
11	301	—						└┴	⊔	8	19	30	└

The effect on the TPIs$_{30}$ of the removal of the multiples of $p_4 = 7$, $p_5 = 11$, $p_6 = 13$, $p_7 = 17$, $p_8 = 19$, $p_9 = 23$, $p_{10} = 29$, and $p_{11} = 31$, is detailed in Appendix D Table. We are particularly interested in TPIs$_{30}$ which have had the TPIs$_{30}$ corresponding to (11, and/or 13), and (17, and/or 19), and (29, and/or (3)1), removed, and whose row values are therefore composite.

Within the initial M_{p_i}, the first of these completely deleted or removed TPIs$_{30}$, (so marked ✕), occurs in respect of the modified response of $M_{17 \times 30}$, at row 13, of Appendix D Table, column (j), and then again at row 17 of the modified response of $M_{17 \times 30}$. The complete removal of a TPI$_{30}$, then propagates along the same row, from the p_i^{th} $M_{p_i \times 30}$, to $M_{p_{i+1} \times 30}$, the p_{i+1}^{th}. Thus, as we use each p_i^{th} $M_{p_i \times 30}$ to remove multiples of each p_i, the opportunity of introduction of more completely deleted or removed TPIs$_{30}$, (✕), is presented.

Now, the set $\mathbb{Z}$ of integers form a Noetherian $\mathbb{Z}$-module (Appendix A, page 10), so we can choose any value $n \in \mathbb{Z}^{+}$ with which to assess the state of the associated list of TPIs_{30}, and we can be assured that the associated number of elements is finite.

We can now begin the proof by way of contradiction.

Proof

Assume that there exists only a finite number of twin primes, and suppose the last twin prime (or set of twin primes if more than one is removed through deletion by the largest respective single prime) is/are removed following division, (so removal of the multiple of a prime), by a prime $p_q \in \mathbb{P}$, $q \in \mathbb{Z}_{>3}$.

Then, since the initial module M_{p_q}, of M_{30}, $M_{p_q \times 30}$, begins with the value p_q, its corresponding TPI_{30} is given by $\times$, and the TPIs_{30} for all values $> p_q$, are composite, so are also given by $\times$.

Hence, noting that for $p_q \geq 31$, each module is always only a single element wide, each row of the initial $M_{p_q \times 30}$, $p_q > 31$, to each $(p_q)^2$, is composite, so contains no twin primes.

Thus, each row of the $M_{p_q \times 30}$, from row 1, to row p_q, have had their twin primes removed, so that all of the TPIs_{30} from row 1, to row p_q, are removed, and so can be marked as $\times$.

But this can never happen.

To see this, recall that initially the TPIs_{30} are unmodified, and all (potential) twin primes are present prior to removal of a prime and its multiples.

Considering the first $M_{p_i \times 30}$, $p_4 = 7-\text{module}$, of M_{30}, $M_{7 \times 30}$, then the maximum number of twin primes able to be removed from the module is 6, since only a maximum of 6 elements can exist in the set of residue classes available for removal or deletion, through division, as multiples of the prime $p_4 = 7$. These are precisely the components $\{[(3)1],[11],[13],[17],[19],[29]\}$.

However, removal of the 6 components cannot take place until component removal in the $p_5 = 11-\text{module}$, of M_{30}, $M_{11 \times 30}$. This is because, for $p_q \geq 31$, only two at most, of the TPIs_{30} components can be removed or deleted in any row of any specific module, and a minimum of 3 TPIs_{30} are required to be deleted, in order to describe modification by way of complete TPIs_{30} removal.

Now, a maximum of 6 $TPIs_{30}$ are pre-modified as the multiple of the prime in the $p_4 = 7-$module, of M_{30}, $M_{7\times 30}$, which leaves all 7 rows free from removed $TPIs_{30}$.

In the next $M_{p_i \times 30}$, given as $p_5 = 11-$module of M_{30}, $M_{11\times 30}$, a maximum of precisely 6 $TPIs_{30}$ are then modified as removed, leaving 5 rows free of any modification.

In the $p_6 = 13-$module, of M_{30}, $M_{13\times 30}$, a maximum of a second 6 $TPIs_{30}$ are pre-modified. In conjunction with the 6 removed $TPIs_{30}$, this leaves 7 $TPIs_{30}$ free from removed $TPIs_{30}$. We can then continue by priming of 6 $TPIs_{30}$ at one stage, (pre-modification) then removal of 6 $TPIs_{30}$ (modification) at the next module stage. We now make the modification process more rigorous.

It is well-known that primes > 3 can be found at positions $6k+1$ and $6k-1$, for specific values of $k \in \mathbb{Z}^+$, and suitable choice of plus or minus one [1]. We have just dealt with the case of $p_5 = 11$, $p_6 = 13 \Leftrightarrow 6k \pm 1$, for $k = 2$. For the case $k = 1$, we have the TP pair $(5, 7)$.

Recalling that only six components at most can be first, pre-modified at each module stage, say at value $6k-1$, then the related maximum of six $TPIs_{30}$ can be modified as removed, at value $6k+1$. Each TP $6k \pm 1$, describes a module of $6k \pm 1$ rows, respectively.

Noting that primes do not exist at every point $k \in \mathbb{Z}^+$, wrt each value $6k \pm 1$, then if they did, each TP pair would be 6 units distance from the previous pair element. Recalling that the maximum number of removed $TPIs_{30}$ is always 6, at every other prime, then if we begin at $p_5 = 11$, with 6 modified $TPIs_{30}$, and 5 free $TPIs_{30}$, then an additional 6 modified $TPIs_{30}$, would be generated every 6 additional units. This would then describe $6(k-1)$ modified $TPIs_{30}$, and 5 free $TPIs_{30}$, wrt each $k = \mathbb{Z}^+$. Similarly, if we begin at $p_6 = 13$, with 6 modified $TPIs_{30}$, 6 pre-modified $TPIs_{30}$, and 1 free $TPIs_{30}$, then this would describe $6(k-1)$ modified $TPIs_{30}$, 6 pre-modified $TPIs_{30}$, and 1 free $TPIs_{30}$, wrt each $k = \mathbb{Z}^+$.

Since the value at which the $TPIs_{30}$ are modified, and pre-modified, do not occur at every point $k \in \mathbb{Z}^+$, then when the 6 modified $TPIs_{30}$ are introduced, the number of $TPIs_{30}$ wrt any prime of a TP, will be $\geq$ the case for $k = \mathbb{Z}^+$, and thus there will occur even more free $TPIs_{30}$ than is indicated for the case of TP primes occurring at every $k = \mathbb{Z}^+$. An example of the growth of modified and removed TPIs$_{30}$ denoted $(\not{6})$, modified but not deleted denoted $(\tilde{6})$, and unmodified TPIs$_{30}$ denoted in standard manner as $n \in \mathbb{N}$, is detailed in the table below.

m	1	2	2	3	3	4	5	5	6	7	...
$6m$	6	12	12	18	18	24	30	30	36	42	...
Prime Module	7	11	13	17	19	23	29	31	37	41	...
	$\tilde{6}$	$\not{6}$	$\not{6}$	$\not{6}$	$\not{6}$	$\not{6}$	$\not{6}$	$\not{6}$	$\not{6}$	$\not{6}$	...
	1	5	$\tilde{6}$	$\not{6}$	$\not{6}$	$\not{6}$	$\not{6}$	$\not{6}$	$\not{6}$	$\not{6}$	...
			1	5	$\tilde{6}$	$\not{6}$	$\not{6}$	$\not{6}$	$\not{6}$	$\not{6}$	...
					1	5	$\tilde{6}$	$\not{6}$	$\not{6}$	$\not{6}$	...
							5	7	$\tilde{6}$	$\not{6}$	...
									7	11	...
										⋮	...

In respect of TPs at every pair, $6k \pm 1$, $k = \mathbb{Z}^+$, or at some pairs $6m \pm 1$, $m \in \mathbb{Z}^+$, there will always exist free, unmodified TPIs$_{30}$ wrt every prime module $M_{p_i \times 30}$, $p_i \geq 7$, and hence the number of TPIs$_{30}$ in any module, will never be depleted.

Hence we can never have all of the TPIs$_{30}$ deleted or removed, in any $M_{p_i \times 30}$, which is our required contradiction.

Thus our original assumption must be in error, and there is not last twin prime.

And hence, there exists an infinite number of twin primes found as pairs of successive odd integers p and $p+2$, for $p, p+2 \in \mathbb{Z}^+$, $p, p+2 \in \mathbb{P}$, the set of primes in canonical ascendance.

Section 6

Computing Primes

Since, when searching for primes, more than one can be found in a single test, it becomes evident that a polynomial solution could be applied in respect of solvation for a finite number of responses. Paying due respect to the Abel-Ruffini theorem, and the Law of Universality of the algorithm, we are forced to accept that, (for calculation of more than 5 solution primes), numerical calculation is likely to be necessary.

Considering the dual pairs $\left(\prod_i p_i - \alpha, \alpha\right)$ of the Folded Number (FN) $FN\left(\prod_i p_i\right)$ it is well-known that we can test the components, using the greatest common denominator $(\gcd(*,*))$ function, in order to determine whether the pair are relatively prime (RP), whence $\gcd\left(\prod_i p_i - \alpha, \alpha\right) = 1$, or whether there exists a common divisor $\gcd\left(\prod_i p_i - \alpha, \alpha\right) = \alpha_k$, such that $\alpha \geq \alpha_k > 1$. The process involved in such a calculation, follows the methodology of solution derivation by way of the Euclidean Algorithm (EA) [1]. Basically the process consists of the repeated subtraction of α, from $\prod_i p_i$, until the result (equal to α_1 say), is such that $1 < \alpha_1 \leq \alpha$. this is followed by the repetition of the residue calculation, using the calculated component α_1, and the initial value α, to generate α_2. The next calculation generates the residue α_3, from the repeated calculation of α_2 minus α_1, and so forth, until we reach the value 1, whence the initial pair $\left(\prod_i p_i - \alpha, \alpha\right)$ are RP, or we reach the value α_k : $1 < \alpha_k \leq \alpha_{k-1}$, for maximum value of k, for which $\gcd\left(\prod_i p_i - \alpha, \alpha\right) = \alpha_k$. Where we begin the process with values formed entirely from as yet undeclared primes, then the result $\gcd\left(\prod_i p_i - \alpha, \alpha\right) = 1$, will describe a new prime, and the result $\gcd\left(\prod_i p_i - \alpha, \alpha\right) = \alpha_k$, for $\alpha \geq \alpha_k > 1$, will describe a product of as yet undeclared primes.

Conducting the lengthy calculation of $\prod_i p_i$, and subsequent construction of the numerical value of length $\geq 10^6$ digits, is a time-consuming process, which can be improved upon via rewriting $\prod_i p_i - k\alpha$, using an adapted form of the EA. Also, rather than continually subtracting the value α from $\prod_i p_i$, and generation of the subsequent residue, we can speed-up the process, via calculation and storage of $\{2,3,\ldots,8,9\}$ times α, and subsequent subtraction from $\prod_i p_i$, and the returned residue of $q_r \alpha \times 10^s$, in which q_r is the digit value closest to the leading r digits of α and the $\alpha -$residue, and s is the number of zeros required in order to pad out the summand. In this way, we would require (excluding calculation of the eight products) as many subtraction calculations as there are number of digits in the queried value.

Calculation of primes in this manner implies difficulties with respect to storage, of the large numbers involved, $\left(\prod_r p_r\right)$ which are currently of the order of a single prime being 10^{15} digits long. However, it cannot be disputed that calculation, in principle, in the sense of a Zeusian computer, (able to complete a calculation immediately), might be made available. For example, the Chinese Remainder Theorem delivers larger solutions than is the case without the theorem, and we, unaided as humans, can provide solutions for much smaller calculations.

A more direct approach, linking empirical computing, and Zeusian calculation, is forwarded by way of Factorial Prime Representation (FPR), $\prod_r p_r$, and its constrained set of divisible and non-divisible factors. The FPR delivers calculation as to primality, using two values only, and the result of their calculation of relative primality. Where the calculation is conducted empirically, there exists a set (region) of solutions in which any calculated (suitable) FPR solution, is prime.

Described in short, the FPR allows calculation of definitive primes, and investigation of primality, via calculation of the relative primality of two values only; this is vastly more speedy than any divisibility algorithm using all of the (suitable) available primes. Current technology supports the calculation of values containing around 10^{15} digits, with the only issues being those of storage of the list of (earlier calculated) primes, and the time of calculation. Pre-storage of the consecutive list of primes allows calculation of FPR EA residues of maximum length no longer than that of the digits of the largest prime divisor of the $\prod_i p_i$. This allows extension of calculation to (very) large primes; much larger than are calculated using current techniques. Prizes are offered currently, for new primes with digits numbering 10^4, 10^5, and 10^6 digits.

A related algorithm can be seen to be accessible, via the FPR $\prod_i p_i = 2.3.5.7.11.13.17.19.23$, and the (prime) value 61, (since $61 < \sqrt{\prod_i p_i}$, and can be viewed as being 'much' larger than the maximum p_i of 23 for example). We would then be interested in the solution to the question 'does $61 \mid \prod_i p_i$, which conceptually, is tested via continuous calculation of $\prod_i p_i - 61k_j$, for various values of k_j, and subsequent application of the EA described on page 32.

In respect of the numerical example described, we would be investigating whether $\prod_i p_i - 61k_i = 0$, or $\prod_i p_i - 61k_i > 0$. Where the calculation equals zero, then 61 contains at least one factor in $\prod_i p_i$, greater than 1, so 61 cannot be prime. Otherwise, 61 is prime, or formed from a product of primes, each larger than the maximum p_i of 23.

Such solvation requires further investigation, and payment of due respect to the magnitude of the final component of the FPR list wrt the FN representation (Appendix B) of our example value of 61,

31	$+ \rightarrow$		αp
30	$- \rightarrow$		βp

such that the $\mathrm{FN}(61) \Rightarrow$ that $\alpha p, \beta p \;\Rightarrow\; p \mid 61$, and $\gcd(\alpha, \beta) = 1$; I.e., p is the largest possible prime divisor of 61, the latter of which is therefore not a prime, unless $p = 61$ (since $p = \pm 1$ is excluded).

The calculation $\gcd\left(\prod_i p_i, \alpha\right)$ is achieved in the following manner, beginning with $p_i = \left[\sqrt{\alpha}\right]^{gp}$, the largest prime $\leq p_i = \left[\sqrt{\alpha}\right]^{g}$, for $[*]^{g}$, the greatest integer function:

Considering $g_1(z) = \prod_i p_i - K\alpha$, then choosing any factor, or list of factors $Q = \prod_q p_q$ say, such that $\prod_i p_i = Q \prod_j p_j$,

then we can remove Q through use of $K = \prod_j p_j + M$,

via $$\prod_i p_i - \left(\prod_j p_j + M\right)\alpha = \prod_i p_i - K\alpha$$

$$\Rightarrow \quad Q\prod_j p_j - \left(\prod_j p_j + M\right)\alpha,$$

$$\Rightarrow \quad (Q - \alpha)\prod_j p_j - M\alpha,$$

$$\Rightarrow \quad Y\prod_j p_j - M\alpha, \text{ for } Y\prod_j p_j \leq M\alpha,$$

We can rewrite this solution as $g_2(z) = \prod_z p_z - M\alpha$, and iterate the process, beginning at line 71, until all of the factors have been used, and the residue generated is given by $g_n(z)$. Following this iterative procedure, and depletion, in any order, of the list of canonically aligned primes, the solution gcd can be found via $\gcd\left(\prod_i p_i, \alpha\right) = \gcd(g_n(z), \alpha)$.

Calculation of primality through use of the multiplication of individual primes, rather than their division into a single value, implies a process utilising simpler calculation, and much less dynamic and passive storage space. Its usefulness is limited to verification of primality, or calculation of a single prime from a product of primes, for large values known to be an unknown prime, or known to be a product of unknown primes.

Each calculation residue generated can be positive or negative, so that, for example, $-61 < \beta < 61 \Leftrightarrow |\beta| < 61, \Rightarrow \left[\sqrt{61}\right]^{gp} = 7$, then $61 \Rightarrow \prod_4 p_4 = 2.3.5.7$. Here we consider the following example, in which, in order to provide clarification of operation, the list of primes utilised is six primes longer than necessary.

The calculation $\gcd\left(\left(\prod_9 p_9 = 2.3.5.7.11.13.17.19.23 = 223092870\right), 61\right)$ follows, in which those values in round brackets are for calculation, and those contained in square brackets $[*]$ are for information only.

From $2.3.5.7.11.13.17.19.23$, and $k.61$, for suitable values of $k \in \mathbb{Z}$,

$$
\begin{aligned}
&\Rightarrow && [2.5.7.11.13.17.19].(3.23 - 1.61) = [2.5.7.11.13.17.19].(8), \\
&\Rightarrow && [5.11.13.17.19].(2.7.8 - 1.61) = [5.11.13.17.19].(51), \text{ or } (|-10|) \\
&\Rightarrow && [5.11.13.17].(19.51 - 15.61) = [5.11.13.17].(54), \text{ or } (|-7|) \\
&\Rightarrow && [5.11.13].(17.54 - 15.61) = [5.11.13].(3), \\
&\Rightarrow && [13].(3.5.11 - 2.61) = [13].(43), \text{ or } (|-18|) \\
&\Rightarrow && (13.43 - 9.61) = [13].(10), \\
& && \text{and } \gcd(10, 61) = (|-1|),
\end{aligned}
$$

and since all primes in $2.3.5.7.11.13.17.19.23$, have been used, and $10 < 61$, then the larger value 61 is prime. Alternatively, if the final $\gcd(*,*)$ is > 1, then it is a factor of the initially examined value 61, which will require verification as to its prime, or composite nature, iteratively, in the manner described.

It has earlier been demonstrated in the Lee-Prime Theorem, Section 2, page 16, that at least one new prime, greater than a largest given prime, can be secured, and made available for computation in the manner described in this section. Thus the $\gcd(*,*)$ calculation of very large values, (relative to the largest generating prime), can be conducted through use of much smaller, related primes. In April 2014, the largest prime computed contained 17,425,170 digits. Computation of the 17,425,170 digit value in the fashion described in this section, would require largest digit prime numbers of the order of 5,000 digits, dynamic memory capacity for calculation of the associated products, of the order of around $10,000,000 - \text{to} - 100,000,000$ digits, and a dedicated area of memory able to calculate the residues of $10,000,000 - \text{to} - 100,000,000$ digit value subtractions.

An alternative approach to verification of primality wrt a value $C \in \mathbb{N}$ say, which is either of, an unknown prime, or a product of unknown primes, can be seen to be satisfied via verification or otherwise, of the composite nature of the given source value C. General testing of primes of the form C, will be seen to be reduced to iterative addition of sequential values $\beta \in \mathbb{N}$, modulo C, and is thus much faster than conventional methods of calculation.

0	1	2	$\cdots$	$m-2$	$m-1$	m	$m+1$	$\cdots$	$\frac{C-5}{2}$	$\frac{C-3}{2}$	$\frac{C-1}{2}$	m
$\frac{C+1}{2}+0$	$\frac{C+1}{2}+1$	$\frac{C+1}{2}+2$	$\cdots$	$\frac{C+1}{2}+m-2$	$\frac{C+1}{2}+m-1$	$\frac{C+1}{2}+m$	$\frac{C+1}{2}+m+1$	$\cdots$	$C-2$	$C-1$	C	$\frac{C+1}{2}+m$
$\frac{C+1}{2}$	$\frac{C+3}{2}$	$\frac{C+5}{2}$	$\cdots$	$C-r-2$	$C-r-1$	$C-r$ $r(r+1)$	$C-r+1$	$\cdots$	$C-2$	$C-1$	C	$C-r$
$\frac{C-1}{2}$	$\frac{C-3}{2}$	$\frac{C-5}{2}$	$\cdots$	$r+2$	$r+1$	r	$r-1$	$\cdots$	2	1	0	r
$\frac{C-1}{2}-0$	$\frac{C-1}{2}-1$	$\frac{C-1}{2}-2$	$\cdots$	$\frac{C-1}{2}-m-2$	$\frac{C-1}{2}-m-1$	$\frac{C+1}{2}-m$	$\frac{C-1}{2}-m+1$	$\cdots$	2	1	0	$\frac{C-1}{2}-m$
$\left(\frac{C-1}{2}\right)^2$	$\left(\frac{C-3}{2}\right)^2$	$\left(\frac{C-5}{2}\right)^2$	$\cdots$	$(r+2)^2$	$(r+1)^2$ 1	r^2	$(r-1)^2$	$\cdots$	2^2	1^2	0^2	r^2
$C-2$	$C-4$	$C-6$	$\cdots$	$2r+3$	$2r+1$	$2r-1$	$2r-3$	$\cdots$	3	1	-1	$2r-1$
C	$C-2$	$C-4$	$\cdots$	$2r+5$	$2r+3$	$2r+1$	$2r-1$	$\cdots$	5	3	1	$2r+1$

In order to begin this process, we can first note from the Table above, some of the fundamental relationships of values contained in any FN row expansion:
The Table entries have been generated wrt the FN C, and its count of individual terms in respect of r, and its mirror value $C-r$, in terms of the pairs $(C-r,r)$. The number of terms $\left(\frac{C+1}{2}\right)$ is counted in the first row, as m terms counted from the left of the table. The row of values above the row of $C-r$, describe the value $C-r$, in terms of its value as a count from $\frac{C+1}{2}$, to m further positive terms, $\frac{C+1}{2}+m$. Similarly, the row of values below the row of r, describe the value r, in terms of its value as a count from $\frac{C-1}{2}$, to m further negative terms, $\frac{C-1}{2}-m$.

The final, and penultimate row of values $2r+1$, and $2r-1$, respectively, both provide an augmented count wrt the row of r. When counted from $r=1$, the former sums to $\left((r+1)^2-1\right)=\sum_{i=1}^{r}(2r+1)$, and the latter sums to $r^2=\sum_{i=1}^{r}(2r-1)$. Information as to the values $r(r+1)$, and 1, in the lower portion of the greyed areas, will be updated in due course.

In order to progress further, we need to consider a composite value C, which can be factored into two components a, and b, each of which is non-trivial, so that $a,b>1$, and RP, whence $\gcd(a,b)=1$.

Thus we have a, and b, each divide C, written $a\,|\,C$, and $b\,|\,C$, whence by the property of Linear Diophantine Equations (LDEs) [1] we can always find values x, and y, such that the values ax, and by, differ by a value of 2, so that $ax-by=2$. The fact that $\gcd(a,b)=1$, implies that C is formed from at least two, distinct primes.

But then we also have $ax.by=abxy=kC\equiv 0 \bmod C$, for $k=xy$.

So that writing $ax=r+2$, and $by=r$, we must have $r(r+2)=kC\equiv 0 \bmod C$.

But this is equivalent to $r(r+1)=(C-r)\bmod C$, the latter of which is contained in the row of $(C-r)$. Further, since $r(r+2)=kC\equiv 0 \bmod C$, then adding the value 1 to both sides, we have $(r+1)^2=r(r+2)+1=kC+1\equiv 1 \bmod C$, so that $(r+1)^2\equiv 1 \bmod C$, the former of which is in the row of r^2. The values modulo C, in the row of r^2, are the Quadratic Residues (Appendix A, page 4). If C is a prime, then all of the columns of the FN, $\mathrm{FN}(C)$, are RP. Hence $r(r+1)$, and r, cannot exist in the same column of a FN, so that we can only have $(r+1)^2\equiv 1 \bmod C$, when $r=0$.

Now writing $\alpha = r+1$, we must also have $r(r+2) = (\alpha-1)(\alpha+1) = kC \equiv 0 \bmod C$, whence $\alpha^2 = kC+1$, $\Rightarrow$ $\alpha^2 \equiv 1 \bmod C$. For k a square, the relation takes the form $\alpha^2 - k^2C = 1$, which can be solved, for solutions $p=\alpha$, $q=k$, in the manner of Pell's equation, through use of the convergents p/q of the continued fraction expansion of $\sqrt{C}$ [1]. However, this detracts from the nature of the integer analysis developed in this work.

We also state the trivial result here, that $m+r = \frac{C-1}{2}$, $\Rightarrow$ $2m+2r+1 = C$, which $\Rightarrow$ $2m+1 \equiv -2r \bmod C$. And since $r(r+2) \equiv 0 \bmod C$, $\Rightarrow$ $r^2 \equiv -2r \bmod C$, so that we also have $2m+1 \equiv r^2 \bmod C$. In addition, substituting $\left(\frac{C-1}{2} - m\right) = r$ in $r(r+2) \equiv 0$ $\Rightarrow$ $m^2 - m - A \equiv 0 \bmod C$ for suitable values of $A \in \mathbb{N}$, so that $m^2 - m - A \equiv r(r+2) \equiv 0 \bmod C$.

We can also note at this point, that $\sum_{i=1}^{m} 2i = m(m+1)$, so that $\sum_{i=1}^{m-1} 2i = m(m-1)$.

Introducing these relationships into the table above, provide the additional details shown in the greyed areas, via $r(r+1) = (C-r) \bmod C$, and $(r+1)^2 \equiv 1 \bmod C$.

Thus, in order to test as to composite nature of a value C containing at least two distinct prime factors, it is enough to verify that for some lower FN row value r, of the FN C, the square of the given value, is congruent to $1 \bmod C$. further, since all squares generated by values of r smaller than $\sqrt{C}$, but greater than 1, are less than C, and thus cannot equal $1 \bmod C$, then the first value $r = 1 \bmod C$, must be $\geq \left[\sqrt{C}\right]^{go}$, the largest odd number $\leq \left[\sqrt{C}\right]^{g}$. Hence we can reduce the initial search region to $\left[\left[\sqrt{C}\right]^{go}, \left(\left[\sqrt{C}\right]^{go}+2\right), \left(\left[\sqrt{C}\right]^{go}+4\right), \ldots, \frac{C-1}{2}\right]$.

We now require a test which deals with powers of a prime p, raised an even power p^{2n}, or raised to an odd power p^{2n+1}, $n \in \mathbb{N}$.

Considering first a prime raised to an even power p^{2n},

then for all $kp^n < p^{2n}$ in the FN p^{2n}, the value kp^n has MF (Section 1, page 4) $p^{2n} - kp^n$. And squaring kp^n generates the value k^2p^{2n}.

But then $p^{2n} \mid k^2p^{2n}$, because $p^{2n} \mid p^{2n}$, which implies that $k^2p^{2n} \equiv 0 \bmod p^{2n}$.

Considering now a prime raised to an odd power p^{2n+1}, then for all $kp^{n+1} < p^{2n+1}$ in the FN p^{2n+1}, the value kp^{n+1} has MF $p^{2n+1} - kp^{n+1}$. And squaring kp^{n+1} generates the value $k^2 p^{2n+2}$.

But then $p^{2n+1} \mid k^2 p^{2n+2}$, because $p^{2n+1} \mid p^{2n+2}$, which implies that $k^2 p^{2n+2} \equiv 0 \bmod p^{2n+1}$.

However, when p is a prime, then the columns of its FN are all RP, so possess no common factor. Hence there does not exist a common divisor, so no square will take the value zero. Hence, in order to test as to composite nature of a value C, formed from only one prime factor p, raised to a power $q \in \mathbb{N}$, p^q, it is enough to verify that for some lower FN row value r, of the FN C, the square of the given value, is congruent to $0 \bmod C$.

Now linking the statements for verification of a composite formed from two or more primes, and a composite formed from a single prime raised to some power, leads to the following theorem, and test:

Lees Prime Summation Theorem

Given a positive integer $p \in \mathbb{P}$,

then the number p is prime if, and only if, $\forall r$:

$r \in \left\{ \left[\sqrt{p}\right]^{go}, \left(\left[\sqrt{p}\right]^{go} + 2\right), \left(\left[\sqrt{p}\right]^{go} + 4\right), \ldots, \frac{p-1}{2} \right\}$, $\left[\sqrt{C}\right]^{go}$ the largest odd integer $\leq \left[\sqrt{C}\right]^{g}$.

we have $r^2 \not\equiv 1 \bmod p$, and $r^2 \not\equiv 0 \bmod p$.

If the test fails for any odd value $\left[\sqrt{p}\right]^{go} + n \leq r \leq \dfrac{p-1}{2}$, $n = \{2, 4, 6, \ldots, \}$ then the number p is composite.

Lees Prime Summation Test

Verification as to the primality of p, via the nature of r^2 modulo p, and Lees Prime Summation Theorem, can be provided through summation in ascendance, of the values $\{1, 3, 5, \ldots, (2r-1), \ldots, (p-2)\}$ modulo p, the sum of which can be conducted from the (odd) value $r = \left[\sqrt{p}\right]^{go}$, the largest odd integer $\leq \left[\sqrt{p}\right]^{g}$. Whence p, is composite, if for any sub-summation of the sum $\left(\sum_{i=1}^{r} (2r-1) = r^2 \right) \bmod p$, is equal to 0, or 1.

Thus verification as to primality can be conducted via modular summation only. This is likely to prove to be a speedy, and efficacious test.

Section 7

Matrices, and the Prime Matrix

Here, we consider the general two-dimensional non-singular matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $a, b, c, d \in \mathbb{Z}^{+}$, and its relation in terms of its similar diagonalised representation using the matrix determinant D, matrix eigenvalues $\lambda = \lambda_i$, for $i = \{1, 2\}$, $\lambda_1 \neq \lambda_2$, and matrix eigenvectors $V_1 = \begin{bmatrix} v_{11} \\ v_{21} \end{bmatrix}$, $V_2 = \begin{bmatrix} v_{12} \\ v_{22} \end{bmatrix}$, for $V = [V_1, V_2]$, so that $A = \frac{1}{D} V \lambda V^{-1}$. Writing this relationship in its elemental form informs us that,

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \frac{1}{D} V \lambda V^{-1} = \frac{1}{v_{11}v_{22} - v_{12}v_{21}} \begin{bmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{bmatrix} \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} \begin{bmatrix} v_{22} & -v_{12} \\ -v_{21} & v_{11} \end{bmatrix}.$$

An accompanying relationship is provided by the Characteristic Equation (CE) $\det(A - \lambda I) = 0$, for I, the identity matrix. The CE $\det\begin{pmatrix} a - \lambda & b \\ c & d - \lambda \end{pmatrix} = 0$, reduces to the general quadratic equation $\lambda^2 - \lambda(a + d) + (ad - bc) = 0$, which can be written in terms of the matrix trace T, and matrix determinant D, as the Characteristic Polynomial (CP) $\lambda^2 - \lambda T + D = 0$, with characteristic root solutions $\lambda = \frac{T}{2} \pm \frac{\sqrt{T^2 - 4D}}{2}$ [2]. We make use of the solution discriminant $T^2 - 4D$, in page 41.

The elemental diagonalised form of the two-dimensional matrix A invites writing of the vector columns V_1, and V_2, in a form likely to assist analysis. We can write the pair of vector columns of V_1, and V_2 respectively, in the following four forms, in which α, and β, are the eigenvector weights corresponding to the eigenvalues λ_1, and λ_2 respectfully:

A). $\begin{bmatrix} 1 \\ \alpha \end{bmatrix} \begin{bmatrix} 1 \\ \beta \end{bmatrix}$ B). $\begin{bmatrix} 1 \\ \alpha \end{bmatrix} \begin{bmatrix} \beta \\ 1 \end{bmatrix}$ C). $\begin{bmatrix} \alpha \\ 1 \end{bmatrix} \begin{bmatrix} 1 \\ \beta \end{bmatrix}$ D). $\begin{bmatrix} \alpha \\ 1 \end{bmatrix} \begin{bmatrix} \beta \\ 1 \end{bmatrix}$.

The simplified form of the elemental diagonalisation generates any of the following respectfully:

A). $$A = \frac{1}{\beta - \alpha} \begin{bmatrix} \beta\lambda_1 - \alpha\lambda_2 & \lambda_2 - \lambda_1 \\ \alpha\beta(\lambda_1 - \lambda_2) & \beta\lambda_2 - \alpha\lambda_1 \end{bmatrix},$$

B). $$A = \frac{1}{1 - \alpha\beta} \begin{bmatrix} \lambda_1 - \alpha\beta\lambda_2 & \beta(\lambda_2 - \lambda_1) \\ \alpha(\lambda_1 - \lambda_2) & \lambda_2 - \alpha\beta\lambda_1 \end{bmatrix},$$

C). $$A = \frac{1}{1-\alpha\beta}\begin{bmatrix} \alpha\beta\lambda_1 - \lambda_2 & \alpha(\lambda_2 - \lambda_1) \\ \beta(\lambda_1 - \lambda_2) & \alpha\beta\lambda_2 - \lambda_1 \end{bmatrix},$$

D). $$A = \frac{1}{\alpha-\beta}\begin{bmatrix} \alpha\lambda_1 - \beta\lambda_2 & \alpha\beta(\lambda_2 - \lambda_1) \\ \lambda_1 - \lambda_2 & \alpha\lambda_2 - \beta\lambda_1 \end{bmatrix},$$

in which $\alpha\beta$ is the eigenvector weight product.

However, it is convenient, and efficient to utilise the vector pair basis $V_1 = \begin{bmatrix} 1 \\ \alpha \end{bmatrix}$, $V_2 = \begin{bmatrix} \beta \\ 1 \end{bmatrix}$, $V = [V_1, V_2]$, so that we are interested in the relationship shown in B, whence

$$\begin{bmatrix} 1 \\ \alpha \end{bmatrix}\begin{bmatrix} \beta \\ 1 \end{bmatrix} \Rightarrow \begin{bmatrix} 1 & \beta \\ \alpha & 1 \end{bmatrix} \Rightarrow \qquad A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \frac{1}{1-\alpha\beta}\begin{bmatrix} \lambda_1 - \alpha\beta\lambda_2 & \beta(\lambda_2 - \lambda_1) \\ \alpha(\lambda_1 - \lambda_2) & \lambda_2 - \alpha\beta\lambda_1 \end{bmatrix}.$$

We can note immediately that $b = \beta(\lambda_2 - \lambda_1)$, and $c = \alpha(\lambda_1 - \lambda_2)$, can be zeroed to $b = 0$, or $c = 0$, via $\beta = 0$, or $\alpha = 0$, respectively. Where necessary, we shall refer to the eigenvalue residue $|\lambda_1 - \lambda_2|$, as the anti-trace, denoted by $\mathcal{T}$. From $\alpha\beta = 0$ via $\beta = 0$, or $\alpha = 0$, we can see that the trace diagonal then becomes equal to the eigenvalues $a = \lambda_1$, and $d = \lambda_2$, respectfully, whence matrix A trace $a + d = \lambda_1 + \lambda_2 = T$, and matrix determinant $D = 1$. We can also note that b, and c, imply the relationship $\frac{b}{c} = -\frac{\beta}{\alpha}$.

From the equation of A above, we have immediately that $b = 0, \Leftrightarrow \beta = 0, \Rightarrow$ a lower triangular matrix (LTM), and $c = 0, \Leftrightarrow \alpha = 0, \Rightarrow$ an upper triangular matrix (UTM). Thus from the matrix formed from the basis pair of eigenvectors $\begin{bmatrix} 1 & \beta \\ \alpha & 1 \end{bmatrix}$, an UTM basis pair of eigenvectors generates an upper triangular design matrix, for which an UTM $\Rightarrow$ another UTM, and similarly, a LTM basis pair of eigenvectors generates a lower triangular design matrix, for which a LTM $\Rightarrow$ another LTM.

Regarding the matrix components $\beta(\lambda_2 - \lambda_1)$, and $\alpha(\lambda_1 - \lambda_2)$, and the invariant eigenvector component residue $(\lambda_1 - \lambda_2)$, then the importance of the eigenvector component residue (weight) products α, and β, is ostensibly apparent. The additional invariant residue $(\lambda_1 - \lambda_2)$, which features in the derived relationship

$$\frac{bc(1-\alpha\beta)^2}{\alpha\beta} = 4D - T^2 = (\lambda_1 - \lambda_2)^2,$$

for the matrix determinant calculated in line 10, with matrix trace $T = a + d$, and matrix determinant $D = ad - bc$, may be as important and useful in analysis as the well-known matrix invariants, D, and T.

Note that in this work, we are particularly interested in non-zero, integer values of $\alpha\beta$, and the corresponding set of solutions wrt the matrix invariant residue T. It is also notable that the matrix anti-trace components b and c, can be described via knowledge of the value of the product pair $\alpha\beta$, and the invariant residue, implying that α, β, and/or their product $\alpha\beta$, may be important qualities in understanding integer matrix properties.

Examining the right-hand-side of the statement $\frac{1}{1-\alpha\beta}\begin{bmatrix} \lambda_1 - \alpha\beta\lambda_2 & \beta(\lambda_2 - \lambda_1) \\ \alpha(\lambda_1 - \lambda_2) & \lambda_2 - \alpha\beta\lambda_1 \end{bmatrix}$, then rewriting the terms in the matrix, and bringing the constant factor $\frac{1}{1-\alpha\beta}$ into the matrix,

delivers the form $\begin{bmatrix} \frac{(\lambda_1 - \lambda_2) + \lambda_2(1-\alpha\beta)}{1-\alpha\beta} & \frac{\beta(\lambda_2 - \lambda_1)}{1-\alpha\beta} \\ \frac{\alpha(\lambda_1 - \lambda_2)}{1-\alpha\beta} & \frac{(\lambda_2 - \lambda_1) + \lambda_1(1-\alpha\beta)}{1-\alpha\beta} \end{bmatrix}$,

which simplifies as $\begin{bmatrix} \frac{(\lambda_1 - \lambda_2)}{1-\alpha\beta} + \lambda_2 & \frac{\beta(\lambda_2 - \lambda_1)}{1-\alpha\beta} \\ \frac{\alpha(\lambda_1 - \lambda_2)}{1-\alpha\beta} & \frac{(\lambda_2 - \lambda_1)}{1-\alpha\beta} + \lambda_1 \end{bmatrix}$.

Now writing the eigenvalue residue per unit determinant distortion, $X = \frac{(\lambda_1 - \lambda_2)}{1-\alpha\beta}$, the matrix simplifies further, so that

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} X + \lambda_2 & -\beta X \\ \alpha X & -X + \lambda_1 \end{bmatrix}.$$

Hence, if an integer factor of the integers λ_1, and λ_2, say ε, also divides X, then matrix A possesses a general integer factor ε, of all matrix terms. We shall term a matrix written in the form $\begin{bmatrix} X + \lambda_2 & -\beta X \\ \alpha X & -X + \lambda_1 \end{bmatrix}$, without a component common factor, as a prime matrix (PM). If neither of $(X + \lambda_2)$, or $(-X + \lambda_1)$ are prime, then we term the matrix as a PM of order zero, denoted PM(0). If only one of $(X + \lambda_2)$, or $(-X + \lambda_1)$ are prime, then we term the matrix as a PM of order one, denoted PM(1). And if both $(X + \lambda_2)$, and $(-X + \lambda_1)$ are prime, then we term the matrix as a PM of order two, denoted PM(2).

Considering now a positive or negative variation in one, or both, of the eigenvalues, the effect of the change on the matrix trace, determinant, and anti-trace, is indicated in the Table below, in which: T_Δ indicates the change in terms of the trace relationship $\Delta\lambda_1 + \Delta\lambda_2$, and $\mathcal{T}_\Delta$ indicates the change in terms of the anti-trace relationship $\Delta\lambda_1 - \Delta\lambda_2$.

$\Delta\lambda_1$	$\Delta\lambda_2$	ΔT	ΔD	$\Delta\mathcal{T}$
+	+	T_Δ	$\lambda_1\Delta\lambda_2 + \lambda_2\Delta\lambda_1$	$\mathcal{T}_\Delta$
+	–	$\mathcal{T}_\Delta$	$-\lambda_1\Delta\lambda_2 + \lambda_2\Delta\lambda_1$	T_Δ
–	+	$-\mathcal{T}_\Delta$	$\lambda_1\Delta\lambda_2 - \lambda_2\Delta\lambda_1$	$-T_\Delta$
–	–	$-T_\Delta$	$-\lambda_1\Delta\lambda_2 - \lambda_2\Delta\lambda_1$	$-\mathcal{T}_\Delta$
+	0	$\Delta\lambda_1$	$\lambda_2\Delta\lambda_1$	$\Delta\lambda_1$
0	+	$\Delta\lambda_2$	$\lambda_1\Delta\lambda_2$	$-\Delta\lambda_2$
–	0	$-\Delta\lambda_1$	$-\lambda_2\Delta\lambda_1$	$-\Delta\lambda_1$
0	–	$-\Delta\lambda_2$	$-\lambda_1\Delta\lambda_2$	$\Delta\lambda_2$

Here, we consider the PM, in respect of a fixed trace and determinant, and unit changes in the weight components α and β, wrt the initial matrix $\begin{bmatrix} 2 & 2 \\ 1 & 3 \end{bmatrix}$, in row A.

	λ_1	λ_2	α	β	$\alpha\beta$	**Original Matrix**	**PM Form**	Δ
A	4	1	1	-2	-2	$\begin{bmatrix} 2 & 2 \\ 1 & 3 \end{bmatrix}$	$\frac{1}{3}\begin{bmatrix} 4+2.1 & -2.(-3) \\ 1.(3) & 1+2.4 \end{bmatrix} = \frac{1}{3}\begin{bmatrix} 6 & 6 \\ 3 & 9 \end{bmatrix}$	Datum
B	4	1	2 **U**	-2	-4	$\begin{bmatrix} 8/5 & 6/5 \\ 6/5 & 17/5 \end{bmatrix}$	$\frac{1}{5}\begin{bmatrix} 4+4.1 & -2.(-3) \\ 2.(3) & 1+4.4 \end{bmatrix} = \frac{1}{5}\begin{bmatrix} 8 & 6 \\ 6 & 17 \end{bmatrix}$	**D D** **U U**
C	4	1	1	-1 **U**	-1	$\begin{bmatrix} 5/2 & 3/2 \\ 3/2 & 5/2 \end{bmatrix}$	$\frac{1}{3}\begin{bmatrix} 4+1.1 & -1.(-3) \\ 1.(3) & 1+1.4 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 5 & 3 \\ 3 & 5 \end{bmatrix}$	**U D** **U D**
d	4	1	0 **D**	-2	0	$\begin{bmatrix} 4 & 6 \\ 0 & 1 \end{bmatrix}$	$-\frac{1}{1}\begin{bmatrix} 4-0 & -2.(-3) \\ 0.(3) & 1-0 \end{bmatrix} = \frac{1}{1}\begin{bmatrix} 4 & 6 \\ 0 & 1 \end{bmatrix}$	**U U** **D D**
D	4	1	-1 **D**	-2	2	$\begin{bmatrix} -2 & -6 \\ 3 & 7 \end{bmatrix}$	$-\frac{1}{1}\begin{bmatrix} 4-2.1 & -2.(-3) \\ -1.(3) & 1-2.4 \end{bmatrix} = -\frac{1}{1}\begin{bmatrix} 2 & 6 \\ -3 & -7 \end{bmatrix}$	**D D** **U U**
E	4	1	1	-3 **D**	-3	$\begin{bmatrix} \frac{7}{4} & \frac{9}{4} \\ \frac{3}{4} & \frac{13}{4} \end{bmatrix}$	$\frac{1}{4}\begin{bmatrix} 4+3.1 & -3.(-3) \\ 1.(3) & 1+3.4 \end{bmatrix} = \frac{1}{4}\begin{bmatrix} 7 & 9 \\ 3 & 13 \end{bmatrix}$	**D U** **D U**

Note in row d, the inclusion of an original matrix entry of zero, generated via a reduction in α, of 1, and its closest relationship in row D, due to a reduction in α, of 2. The final colum indicates the increase (U) or decrease (D) generated wrt the original matrix, and its subsequently produced PM form. Only those matrices in rows A, and D, are PMs, with both being PM(2).

Since the matrix entry values a,b,c,d, exclude the value zero, then there are precisely 15 other dedicated forms of response, some of which may be repeated in terms of unit (or 2 units, since the value 0 is excluded) increase or decrease of each of the four components, corresponding to the four regions $(+x,+y)$, $(+x,-y)$, $(-x,+y)$, $(-x,-y)$. The 16 different general locations can be counted as the sum of those locations with no negative values, one negative value, two negative values, three negative values, and four negative values respectively, ${}^4C_0+{}^4C_1+{}^4C_2+{}^4C_3+{}^4C_4 \Rightarrow 1+4+6+4+1=16$.

Investigative analysis can proceed via equating $r:1<r<4$ of the 4 matrix options, or via equating any of the components to a prime, or a product of primes. Further, noting that for p prime, $p=\lambda_1-\alpha\beta\lambda_2$, we have $(1-\alpha\beta)\nmid p=(\lambda_1-\alpha\beta\lambda_2)$, unless $(1-\alpha\beta)=\pm p$, whence $\alpha\beta=(1\pm p)$, $p\in\mathbb{P}$. This is similar to the case for p composite, except that $(1-\alpha\beta)$ also divides $p=(\lambda_1-\alpha\beta\lambda_2)$, for at least two values: $-p<(1-\alpha\beta)<p$, $\alpha\beta\neq 1$. The set of PM-viable integer matrix entries, forwards the set of ordered integer quadruples of $\mathbb{Z}^4=\{\,(a,b,c,d),\ a,b,c,d\in\mathbb{Z}^+\,\}$, from which we can produce the PM-applicable functions

$$\mathrm{T}:\ \mathbb{Z}^4\rightarrow\ \mathbb{Z}^4$$

$$x_i\mapsto\frac{x_i}{q_i p},\quad q_i=\left\{q_i:q_i\mid\frac{x_i}{p}\right\},\quad i=\{1,2,3,4\},\ x_1=a,\ x_2=b,\ x_3=c,\ x_4=d,\ p\ \text{a prime},$$

which describes the set of composite PMs with entries $x_i=q_ipk_i$, $k_i\in\mathbb{Z}$, in which three of the q_i, at most, can be equal to 1, and

$$\Gamma:\ \mathbb{Z}^4\rightarrow\ \mathbb{Z}^4$$

$$x_i\mapsto\frac{x_i}{p},\quad i=\{1,2,3,4\},\ x_1=a,\ x_2=b,\ x_3=c,\ x_4=d,\ p\ \text{a prime},$$

which describes the set of prime PMs with entries $x_i=pk_i$, $k_i\in\mathbb{Z}$.

Thus the PM is able to discern between sets of four composites, and sets of four relatively prime components.

For fractional $\alpha\beta : \alpha\beta = \frac{n}{n+1}$, $n = \mathbb{N}$, matrix generation using an initial FN pair as the initial trace value $\lambda_1 + \lambda_2$, is an automorphic function (Appendix A, page 6) into the set of FN pairs corresponding to the initial FN pair (Appendix B). For example, from 35, $\Rightarrow$

r	0	1	2	$\cdots$	
λ_{1_i}	18	19	20	$\cdots$	$\underset{\to\infty}{(*)+1}$
λ_{2_i}	17	16	15	$\cdots$	$\underset{\to-\infty}{(*)-1}$

105 and $\lambda_1 = 18,\ \lambda_2 = 17, \Rightarrow \begin{bmatrix} 17 + \frac{1}{1-\alpha\beta} & \frac{-\beta}{1-\alpha\beta} \\ \frac{\alpha}{1-\alpha\beta} & 18 - \frac{1}{1-\alpha\beta} \end{bmatrix} = \begin{bmatrix} 18+n & -1\beta \\ 1\alpha & 17-n \end{bmatrix},$

we have

$$\frac{0}{1} \Rightarrow \begin{bmatrix} 18 & -1\beta \\ 1\alpha & 17 \end{bmatrix}, \qquad \frac{1}{2} \Rightarrow \begin{bmatrix} 19 & -2\beta \\ 2\alpha & 16 \end{bmatrix},$$

$$\frac{2}{3} \Rightarrow \begin{bmatrix} 20 & -3\beta \\ 3\alpha & 15 \end{bmatrix}, \qquad \frac{3}{4} \Rightarrow \begin{bmatrix} 21 & -3\beta \\ 3\alpha & 14 \end{bmatrix},$$

and in general,

$$\frac{r}{r+1} \Rightarrow \begin{bmatrix} \frac{(\lambda_1+\lambda_2)+1}{2} + r & -(r+1)\beta \\ (r+1)\alpha & \frac{(\lambda_1+\lambda_2)-1}{2} - r \end{bmatrix}, \quad r = \mathbb{N}.$$

Section 8

Quantum Space

Mathematical Physics provides for a description of a coordinate system with space co-ordinates $(x, y, z) \in \mathbb{R}^3$, and time t, supporting a space-time diagram via the $4-$dimensional system (x, y, z, t). Utilising the $4-$component system, we can examine an arbitrary space component A, in respect of the quantum nature of space.

The (naïve) spatial position $A = (x, y, z)$, coupled with time t, is termed an event. It is required to support the location of mass, or energy, of unknown quantities. The nature of mass and/or energy, implies that the respective position $A = (x, y, z, t)$ is not an isolated point, implying its continuity. The paths of particles or energy in a space-time diagram are termed space-time curves, or world-lines. In this brief, we consider the spatial coordinate of the two-dimensional system (x, t), in which the $x-$axis is usually the horizontal axis.

Consideration of the wave nature of particles, implies that there exists a fundamental limit to the knowledge of the energy of a particle when it is measured for a finite time. This is one facet of the Heisenberg Uncertainty Principle (HUP); the other being the uncertainty of precision of a particle's position coordinate, and its momentum. In both statements, the product of the uncertainties in the corresponding measurements of each, must be $> \hbar$, Planck's constant h, normalised by 2π. Thus, HUP, and the nature of mass and energy, support the principle of a (suitably large) finite, or infinite, number of smears of mass or energy, at any spatial position A. In this brief, we imply that the number of smears of mass or energy in the quantum space state, is > 8.

The relationship between the quantum nature of space, and that of any smears of dual located mass or energy, and considerations of the operation or function of dual physical constructs in space, supporting the existence of a non-isolated point, implies the minimisation and stability, of mass or energy, at spatial points of resonance, where such can be found.

In order to demonstrate the relationship between the quantum nature of space, and the quantum nature of the physical world, we require the following statement:

Lee's Equation

The triple implication

$$(x + y) = (z + c)$$

$$\Leftrightarrow \qquad\qquad \Leftrightarrow$$

$$2(xy - zc) = c^2 \quad \Leftrightarrow \quad x^2 + y^2 = z^2$$

Dennis Lee

is true $\forall x, y, z, c \in \mathbb{N}$, such that x, y, z support a Pythagorean triangle $x^2 + y^2 = z^2$.

The proof proceeds by construction.

Consider the case

$\exists x, y, z, c \in \mathbb{N}$: $\quad (x+y) = (z+c)$ 1

$\Leftrightarrow \quad (x+y)^2 = (z+c)^2$

$\Leftrightarrow \quad 2(xy - zc) = z^2 - x^2 - y^2 + c^2,$ 2

so that using Proof by Cases, $\Rightarrow$

$$x^2 + y^2 = z^2 \quad \Leftrightarrow \quad c^2 = 2(xy - zc). \qquad 3$$

Now, working in another direction in order to provide a triangular implication from

$$c^2 = 2(xy - zc), \qquad 4$$

$\Leftrightarrow \quad c^2 + 2zc - 2xy = 0.$

Solving the quadratic in $'c'$

$\Leftrightarrow \quad c = -z \pm \sqrt{z^2 + 2xy},$ 5

$\Leftrightarrow \quad z + c = \pm\sqrt{z^2 + 2xy}.$

Squaring

$\Leftrightarrow \quad (z+c)^2 = z^2 + 2xy,$ 6

and completing the square

$\Leftrightarrow \quad (z+c)^2 - (x+y)^2 + x^2 + y^2 = z^2,$

So that again, using Proof by Cases

$\Leftrightarrow \quad (x+y) = (z+c) \quad \Leftrightarrow \quad x^2 + y^2 = z^2.$ 7

Also, for all Pythagorean triangles $x^2 + y^2 = z^2$, $\quad x, y, z, c \in \mathbb{N}$, then

$$x^2 + y^2 = z^2 \quad \Leftrightarrow \quad (x+y)^2 - 2xy = (z+c)^2 - 2zc - c^2,$$

so that Proof by Cases $\Rightarrow$

$$(x+y)^2 = (z+c)^2 \quad \Leftrightarrow \quad c^2 = 2(xy - zc). \qquad 8$$

Thus, combining the implications provides that

	$(x+y) = (z+c)$	
$\Leftrightarrow$		$\Leftrightarrow$
$2(xy - zc) = c^2$	$\Leftrightarrow$	$x^2 + y^2 = z^2$

as required.

Returning now to the physical, spatial analogy, an arbitrary point a, along the $x-$axis, can describe any value $a \in \mathbb{R}$, and thus supports the co-existing, corresponding $2-$partition element $a = (x+y) = (z+c)$, in which all of the components operate along the $x-$axis, and $a, x, y, z, c \in \mathbb{R}$. This implies that a result generated through application of Lee's Equation, may be applicable throughout the (stable) domains of space, mass, and energy.

In general Physics, an orbital is defined to be the space-dependent part of a wavefunction for an electron in an atom. The wavefunction is a probalistic function dealing with describing the location of an electron in a particular region surrounding the atomic nucleus. It is specified through the use of four quantum numbers; the principal quantum number n, the orbital angular momentum number l, the magnetic angular momentum number m_l, and the magnetic spin number m_s. There are up to n of the l, $2l+1$ of the m_l, and 2 of the m_s. The state of any electron is then given through defining its orbitals, subject to the Pauli Exclusion Principle (PEP), which governs the manner in which electrons can fill the available orbitals. For particular values of l, and m_l, solutions of the wavefunction described by the Schrödinger Equation, are well-behaved only when the energy is quantized, implying an integer value of n.

One result generated through application of Lee's Equation, deals with the generation of stable regions of space corresponding to stable regions of mass or energy. In order to see this, we first need to rewrite the relationship $c^2 = 2(xy - zc)$ from Lee's Equation, in a suitable form, so that

$$\frac{c^2}{2} = (xy - zc), \qquad 9$$

$$\Leftrightarrow \qquad xy = \frac{c^2}{2} + zc = \frac{c(c+2z)}{2},$$

$$\Leftrightarrow \qquad xy = \frac{c(2c+2z-c)}{2} = \frac{c(2(x+y)-c)}{2},$$

$$\Leftrightarrow \qquad xy = c(x+y) - \frac{c^2}{2}, \qquad 10$$

$$\Leftrightarrow \qquad x(y-c) = \frac{2cy - c^2}{2},$$

$$\Leftrightarrow \qquad x = \frac{c(2y-2c+c)}{2(y-c)},$$

$$\Leftrightarrow \qquad x = c + \frac{c^2/2}{y-c}. \qquad 11$$

This equation, which supports the generation of all Pythagorean triangles, and $\Rightarrow x, y, z, c \in \mathbb{N}$, takes integer solutions precisely when $(y-c)$ is a positive factor of $c^2/2$.

Noting first that c is necessarily even, we can construct the following table, in which $c^2/2 = 2n^2$, and $\sqrt{(xy-zc)} = n\sqrt{2}$.

n	c	c^2	$c^2/2$	$\sqrt{c^2/2}$	Factors	Factor No.	Shell
1	2	4	2	$\sqrt{2}$	1, 2	2	K
2	4	16	8	$2\sqrt{2}$	1, 2, 4, 8	4	L
3	6	36	18	$3\sqrt{2}$	1, 2, 3, 6, 9, 18	6	M
4	8	64	32	$4\sqrt{2}$	1, 2, 4, 8, 16, 32	6	N
5	10	100	50	$5\sqrt{2}$	1, 2, 5, 10, 25, 50	6	O
6	12	144	72	$6\sqrt{2}$	1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, 72	12	P
7	14	196	98	$7\sqrt{2}$	1, 2, 7, 14, 49, 98	6	Q
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

Since the factors 1 and 2 always exist as factors, for $n \to \infty$, we can be assured that the entire set of Pythagorean triangles is generated. Examining the related Pythagorean triangles $\Rightarrow$

$c = 2 \Rightarrow x = 2 + \dfrac{2}{y-2} \Rightarrow$ the two integer factor solutions $1, \& 2$, so that

$y = 3, x = 4, z = 5$; and $y = 4, x = 3, z = 5$.

$c = 4 \Rightarrow x = 4 + \dfrac{2}{y-4} \Rightarrow$ the four integer factor solutions $1, 2, 4, \& 8$, so that

$y = 5, x = 12, z = 13$; $\quad y = 6, x = 8, z = 10$; $\quad y = 8, x = 6, z = 10$; and $y = 12, x = 5, z = 13$.

Etc. ....

Regarding the Table entry spatial properties, the integer values of n, correspond to the principal quantum number and the physical electron shells K, L, M, N, O, P, Q, and the value

$c^2/_2 = (xy - zc) = 2n^2$ at each n, describes the maximum number of orbitals allowable in any corresponding electron shell, wrt the total number of the associated group of quantum numbers. However, for $n > 4$, the maximum number of electrons indicated is not reached in the physical domain. Further support is provided to the set of Lee's Equation-defined, shell maximum orbital numbers $\{2, 8, 18, 32, 50, 72, 98\}$, corresponding to the number of protons in any particular atom, through their generation of a sigma-algebra-related basis for the set of magic numbers of atomic theory, $\{2, 8, 20, 28, 50, 82, 126\}$, at which the corresponding number of protons (or neutrons) in an atomic nucleus is the most stable. For example, one such relation, via the stable equipartition of energy, might be:

$\{2,\ \ 8,\ \ 20 = 2 + 18,\ \ 28 = 2 + 8 + 18,\ \ 50 = 18 + 32,\ \ 82 = 32 + 50,\ \ 126 = 28 + 98\}$.

Further properties require clarification.

The Fermat-Lee Theorem

In this work, we demonstrate a possibility for the 'wonderful proof', mentioned by Fermat, as not being able to fit into the margin. It is 'wonderful', in the sense that it is simple, and precise. It is left to the reader to decide whether this is indeed the proof described by Fermat.

Proof that we cannot secure a solution in the integers, wrt $x^n + y^n = z^n$, for $x, y, z \in \mathbb{Z}^+$, $n > 2$, $n \in \mathbb{Z}^+$, is assisted via proof of the impossibility of solving $x^4 + y^4 = z^2$, which is a prerequisite for the proof that $x^4 + y^4 = z^4$. The latter caters for the case of n even, and containing no odd prime factors. We then note that if n contains an odd prime factor p, so that $n = kp$, the equation $x^n + y^n = z^n$, can be written as $(x^k)^p + (y^k)^p = (z^k)^p$. One can also note that we must always have x even, y, z odd, $\gcd(x, y, z) = 1$ [1]. Hence it will suffice to prove the case for $n > 2$, $n \in \mathbb{P}$, the set of primes in canonical ascendance, $n = p_i :\ p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ \ldots, p_i, \ldots,$.

Theorem

There exist no positive integers $x, y, z \in \mathbb{Z}^+$, x even, y, z odd, $\gcd(x, y, z) = 1$ satisfying the relationship

$$x^n + y^n = z^n, \tag{1}$$

for $n > 2$, $n \in \mathbb{P}$, the set of primes in canonical ascendance, $n = p_i :\ p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ \ldots, p_i, \ldots,$

Lee's Theorem

Before beginning, we note that Lee's theorem provides that for $x, y, z \in \mathbb{Z}^+$, and $n = 2$, we have

$$\boxed{\begin{array}{ccc} & (x+y) = (z+c) & \\ \Leftrightarrow & & \Leftrightarrow \\ 2(xy - zc) = c^2 & \Leftrightarrow & x^2 + y^2 = z^2 \end{array}} \tag{2}$$

which also delivers the set of Pythagorean triangles.

Proof

The proof proceeds by construction of a general property of the binomial expansion of $(x + y)$, assumption of a related hypothesis, and its subsequent contradiction.

Suppose a solution exists for any odd value of $n > 2$, $n \in \mathbb{P}$, satisfying $x^n + y^n = z^n$.

Then we have

$$(x+y)=(z+c), \tag{3}$$

whence the laws of binomial expansion provide that,

$$(x+y)^n=(z+c)^n \tag{4}$$

is true for some positive integer $c \in \mathbb{Z}^+$.

In the expansion of the LHS of Eqn. 4, as

$$\binom{n}{0}x^n+\binom{n}{1}x^{n-1}y+\ldots+\binom{n}{r}x^{n-r}y^r+\ldots+\binom{n}{n-1}xy^{n-1}+\binom{n}{n}y^n, \tag{5}$$

for any odd positive integer $n>2$, $n \in \mathbb{P}$, and $\binom{n}{r}=\frac{n!}{r!(n-r)!}$, there are an even number of terms, paired as the two terms containing $\binom{n}{r}$, $\binom{n}{n-r}$, centred about the pair $\binom{n}{\frac{n-1}{2}}$, $\binom{n}{\frac{n+1}{2}}$.

This means that we can write each pair $\binom{n}{r}x^{n-r}y^r$, and $\binom{n}{n-r}x^r y^{n-r}$, $0<r<n$, as

$$\binom{n}{r}x^r y^r\left(x^{n-2r}+y^{n-2r}\right). \tag{6}$$

Thus for $n>2$, $0<r<n$, and equating Eqn. 4, with the RHS of Eqn. 3,

$$\binom{n}{0}z^n+\binom{n}{1}z^{n-1}c+\ldots+\binom{n}{r}z^{n-r}c^r+\ldots+\binom{n}{n-1}zc^{n-1}+\binom{n}{n}c^n, \tag{7}$$

we have, for $x^n+y^n=z^n$,

$$c^n=\sum_{r=1}^{\frac{n-1}{2}}\binom{n}{r}\left(x^r y^r\left(x^{n-2r}+y^{n-2r}\right)-z^r c^r\left(z^{n-2r}+c^{n-2r}\right)\right). \tag{8}$$

Continuing the process iteratively, using each $\left(x^{n-2r}+y^{n-2r}\right)$, implies that each term can be written as a product of $(x+y)$. Similarly, each term in $\left(z^{n-2r}+z^{n-2r}\right)$, can be written as a product of $(z+c)$.

Then writing $(x+y)=(z+c)$, we have that c^n is divisible by $(z+c)$.

But this $\Rightarrow$ $c \mid z$.

But z is odd, and this can never happen in the positive integers.

Hence for each $n > 2$, $n \in \mathbb{P}$, $x^n + y^n = z^n$ is false for $x, y, z \in \mathbb{Z}^+$.

Q.E.D.

For example, using the Binomial Theorem, we have:

$x^3 + y^3 =$

$$(x+y)^3 - 3x^2y - 3xy^2 = (x+y)^3 - 3xy(x+y) = (x+y)f_3(x,y),$$

for related 3-D Binomial Theorem expansion residue $f_3(x,y)$, and

$x^5 + y^5 =$

$$(x+y)^5 - 5x^4y - 5xy^4 - 10x^3y^2 - 10x^2y^3 = (x+y)^5 - 5xy(x^3+y^3) - 10x^2y^2(x+y)$$

$$= (x+y)^5 - 5xy(x+y)f_3(x,y) - 10x^2y^2(x+y)$$

$= (x+y)f_5(x,y),$

for related 5-D Binomial Theorem expansion residue $f_5(x,y)$.

Then from $(z+c) = (x+y)$, we have similarly,

$$z^5 + c^5 = (z+c)f_5(z,c).$$

Hence from $(x+y) = (z+c)$, we have

$$(x+y)^5 = (z+c)^5,$$

So that we have

$$(x+y)^5 - 5x^4y - 5xy^4 - 10x^3y^2 - 10x^2y^3 = (z+c)^5 - 5z^4c - 5zc^4 - 10z^3c^2 - 10z^2c^3.$$

Suppose $x^5 + y^5 = z^5$, is true under the specified conditions, then its elimination provides that

$$(x+y)f_5(x,y) = c^5 + (z+c)f_5(z,c) \Rightarrow c^5 = (x+y)f_5(x,y) - (z+c)f_5(z,c).$$

But since $(z+c) = (x+y)$, we can rewrite this as

$$c^5 = (z+c)f_5(x,y) - (z+c)f_5(z,c). \Rightarrow c^5 = (z+c)(f_5(x,y) - f_5(z,c)).$$

But then this implies that $(z+c) \mid c^5, \Rightarrow c \mid z$.

However, since z is odd, whilst c is even, this cannot be true, which provides our required contradiction.

Hence $x^5 + y^5 = z^5$, for $x, y, z \in \mathbb{Z}^+$, cannot be true. Higher order cases are similar.

References: [1]. *Elementary Number Theory*, Revised printing, **1988**, D.M. Burton.

APPENDIX

A: Rings, Fields, Ideals, and Modules

The numerical elements dealt with in this work are the numbers expressible as the sum or difference of any two natural numbers $\mathbb{N} = \{1, 2, \ldots\}$, described as the set of integers $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$. The integers are also known as (aka) signed numbers or directed numbers, and are recognized as being the set of rational numbers $\mathbb{Q}$, able to be expressed as a ratio of integers a/b, for a, b in their lowest form, (in which $b \neq 0$, and is usually non − negative), such that the denominator $b = 1$. Modifications of the numerical sets, such as $\mathbb{N}^0 = \{0, 1, 2, \ldots,\}$, the set of non-negative integers, and $\mathbb{Z}^+ = \{1, 2, \ldots,\}$, the set of positive integers exist.

A set, or class of numerical objects is a collective list of the elements, and is usually denoted by encapsulation within braces $\{\ \}$, aka curly brackets. The list of elements in a set does not require declaration; so $\{1, 2, 3, 4\}$ is a set, as is $\{a, b, c, d\}$. Both of the sets shown, are sets of 4 objects. The study of sets/classes, and their relations, is known as set theory. Sets and subsets can be described as measures possessing the property of countable additivity, through the definition of appropriate set functions operating on the set. The best known of these measures, incorporates the sigma-algebra (σ − algebra); denoting a set of elements containing itself, the empty set ($\emptyset$), the complements of all set member collections, and the countable union of all set members; in conjunction with Boolean Algebra. The resulting synthesis is known as Boolean Sigma-Algebra. The Boolean nature indicated here describes the operations of complement (A/B), (in which B is the complement of A), union ($\bigcup$), and intersection ($\bigcap$), as described by George Boole's (1815~1864) Algebra of Classes/Sets. A Boolean Sigma-Algebra with a measure, is known as a measure algebra, or field of sets.

The set of real numbers $\mathbb{R}$ include irrational expressions and fractional powers. Together with the set of integers $\mathbb{Z}$, and set of rationals $\mathbb{Q}$, they are examples of structured sets which satisfy specific criteria. For example, the sets $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$, each satisfy the triangle inequality, that the sum of any two sides of a triangle measurable by $\mathbb{Z}$, $\mathbb{Q}$, or $\mathbb{R}$ respectively, is greater than the third. A fundamental relationship in number theory provides that for any two natural numbers $a \geq b,\ a, b \in \mathbb{N}$, there exists $(\exists)$ two unique values $q, r \in \mathbb{N}$, such that

$$a = qb + r, \qquad 0 \leq r < b. \qquad (1)$$

This is the division algorithm. This means that given a base b, then $r = \{0, 1, 2, \ldots, b-1\}$, and q multiplies the value b. Regarding the fraction or ratio $a/_b$, and its representation as a division algorithm, then q is the quotient, and r is the remainder or residue. Thus any positive integer in $\mathbb{Z}^+$ can be represented as a product q of any other number b, plus a remainder r, which is less than the value b.

An extension to arithmetic, termed modular arithmetic, utilizes the base b, (aka the modulus of the system), in order to represent any given number a, in the division algorithm, as the remainder r, and modulus, (or more commonly modulo, or mod) b. This is written as

$$a \equiv r \bmod b, \quad \text{or} \quad a \equiv_b r, \qquad (2)$$

read as 'a is congruent to $r \bmod b$', or 'a is congruent $\bmod b$, to r', where r is the remainder or residue. Mod is short for modulo, which means 'to the modulus'. Thus, a is congruent to r modulo b, if $(a-r)$ is a multiple of b. Systems demonstrating modular arithmetic, denoted $\mathbb{Z}_n$ for finite modulus n, submit to the operations of addition $(+)$, and multiplication $(.)$, in their natural sense, so that

$$a \equiv_b r, \quad c \equiv_b s \quad \Leftrightarrow \quad (a+c) \equiv_b (r+s), \quad \text{where} \quad r+s < b,$$

$$\text{and} \qquad (3)$$

$$a.c \equiv_b r.s, \quad \text{where} \quad r.s < b.$$

Considering the modular arithmetic statement $a \equiv r \bmod b,\ a \in \mathbb{Z}$, then there are an infinite number of values a, generating the residue r. For example, in $a \equiv 2 \bmod 3$, then $a = \{\ldots, -7, -4, -1, 2, 5, 8, \ldots\}$, whilst the residue is equal to 2. Thus in the integers, the residue is the (integer) remainder $r \in \{0, 1, \ldots, b-1\}$ upon division by the (integer) base b. This defines modular arithmetic, modulo b.

The set of numerical components S encapsulating modular arithmetic, modulo n, satisfy requirements for 3 specific operations of the binary relation on the set S, together termed an equivalence relation, denoted $(S,\sim)$. The elements are: Reflexive, so that an element is related to itself; Symmetric, thus relating it to another set element; and Transitive, so that similar symmetric images and ranges are related to differing symmetric ranges and images, respectively. A set together with its equivalence relation $(\sim)$, is termed a Setoid, written $(S,\sim)$, or $\widetilde{S}$. When the (usually) finite set, (aka class), of elements S, satisfies requirements for an equivalence relation, the equivalence class $[a]$ denotes the set of elements of S that are equivalent to a, so that

$$[a] \equiv \{x : x \in S, \text{ and } a \sim x\}. \qquad (4)$$

The collection of equivalence classes are disjoint and exhaustive on the set S, and constitutes a partition of the set S.

A residue class, or congruence class $[a]$, is an equivalence class for the equivalence relation of congruence modulo n. Any two integers belong to the same class if and only (iff or $\Leftrightarrow$) they possess the same remainder, a, upon division by n. Arithmetic can be defined in the residue classes as

$$[a]+[b]=[a+b], \quad [a][b]=[ab], \quad a,b \in \{0, 1, 2, \ldots, n-1\}. \qquad (5)$$

Representation of modular classes is usually via the least non-negative member. The set of residue classes mod n, is given by the set $\{m : m = a + kn\}$: $0 \le a \le n-1$ is a residue mod n, and k is a non-negative integer. The class of least residues is an example of a complete residue system modulo n, containing one element from each class. The set of least residues is a partition containing the smallest element in each class. The set of least absolute residues is the complete set of residues satisfying $-\frac{n}{2} < a_k < \frac{n}{2}$, $\quad k = \{1, 2, \ldots, n\}$. The Reduced residue system modulo n, contains one element from each class relatively prime to n; I.e. $\{1, 3, 5, 7\}$ is the reduced residue system mod 8. For $n \in \mathbb{Z}^+$ the number of positive integers $\mathbb{Z}^+ < n$, relatively prime to n, is given by Eulers function, denoted $\varphi(n)$, aka the Euler Phi function, aka the Totient. It counts the number of distinct reduced residue classes of an integer via its prime powers, so that $\varphi(p^{k+1}) = p^k(p-1)$. Euler extended his Phi function, to be a special case of Fermats Little Theorem that for any $n \in \mathbb{Z}$, and $p \in$ the set of primes $\mathbb{P}$ in ascending canonical order, $p_1 = 2$, $p_2 = 3$, $p_3 = 5, \ldots : p \nmid n$, $n \equiv 1 \pmod{p}$, via $\forall a \in \mathbb{Z}$, $\gcd(a,n) = 1$, $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Other well-known number-theoretic functions include $\tau(n)$, the number of positive divisors of n, $\sum_{d|n} 1$, and $\sigma(n)$, the sum of the positive divisors of n, $\sum_{d|n} d$. A function $f(\ )$ is termed multiplicative if $\gcd(x,y)=1$, and $f(xy)=f(x)f(y)$. The functions $\tau(n)$, $\sigma(n)$, Eulers Phi function, and the Legendre symbol, are all examples of multiplicative functions. For example, when p is a product of not necessarily distinct odd primes p_i, then the Legendre symbol $(a/p)=(a/p_1).(a/p_2).\dots.(a/p_n)$, is a multiplicative function, termed the Jacobi symbol.

Equations, and relationships, $f(x)(\mathrm{mod}\, m)$, can be posed in modular arithmetic, and solutions, where possible, provided. In general, a congruence equation seeks solution(s) to

$$f(x)\equiv 0(\mathrm{mod}\, m) \quad \text{or} \quad f(x)\equiv_m 0, \qquad (6)$$

where $f(x)$ is a polynomial with integer coefficients, aka an integral polynomial, which can be linear, quadratic, or of higher order. In order to locate a solution to a congruence equation, only a complete set of residues need be considered. The linear congruence equation $ax\equiv b(\mathrm{mod}\, n)$ is soluble $\Leftrightarrow$ $\gcd(a,n)\,|\,b$. In a quadratic congruence equation, $f(x)$ is a quadratic polynomial, mod n. A number a, congruent modulo n to a perfect square, describes a quadratic residue. For $p\in\mathbb{P}$, $2\nmid p$, the quadratic residues are congruent to $1^2, 2^2, 3^2, \dots, \left(\frac{p-1}{2}\right)^2$, so that $x^2\equiv a(\mathrm{mod}\, n)$ say, is termed a quadratic residue $(\mathrm{mod}\, n)$. When n is prime, then $n=p\in\mathbb{P}$, and $x^2\equiv a(\mathrm{mod}\, p)$ is valid when, for $\gcd(a,p)=1$, the Legendre symbol $a/p=1$ (This is also written $a\,|\,p=1$, but can then be mistaken for divisibility). If $\gcd(a,p)\neq 1$, then $a/p=-1$. By Eulers Criterion, for p an odd prime, $a/p\equiv a^{\left[\frac{p-1}{2}\right]}(\mathrm{mod}\, p)$, whilst for p even, $2/p\equiv -1^{\left[\frac{p^2-1}{8}\right]}(\mathrm{mod}\, p)$.

Returning to sets of elements, the notion and application of sets can be refined to that of groups, through a requirement for all related set objects to conform to a collective of specific requirements. These are:

Closure: The smallest closed set containing the intersection of all closed sets of the solution set. The sets are refined via adherence to closure under the operation $\circ$, such that in consideration of a group G, the operation $\circ$ satisfies

(1) Association: $\forall a,b,c\in \mathrm{G}=\{*\}$, $a\circ(b\circ c)=(a\circ b)\circ c$,

(2) Identity: $\exists\, e \in \mathrm{G}: \quad a \circ e = e \circ a = a, \ \forall a \in \mathrm{G},$

(3) Inverse: $\forall a \in \mathrm{G}, \ \exists\, a' \in \mathrm{G}: \quad a \circ a' = a' \circ a = e.$

Groups can be denoted $(\mathrm{G}\ ,\ \circ)$, or $\langle \mathrm{G}, \circ \rangle$, with appropriate clarification of operation $\circ$. Examples of groups include; the set of integers under addition, $(\mathbb{Z},\ +)$; the set of real numbers under addition, $(\mathbb{R},+)$; the set of complex numbers (excluding zero) under multiplication, $(\mathbb{C}_{\{0\}},\cdot)$ or $(\mathbb{C}_{\{0\}},\ \times)$; the set of real 2×2 matrices under addition $(\mathrm{M}_{2\times2}\ ,\ +)$; and the set of vectors in 3-D space, under addition $(\mathrm{V}_{3\mathrm{D}}\ ,+)$. If H is a subset of G forming a group under operation $\circ$, then H is a subgroup of G. For instance $\{1, i, -1, -i\}$ is a subgroup $(\{1, i, -1, -i\}, \times)$ of $(\mathbb{C}_{\{0\}},\times)$.

Many collections of objects are not as well-defined as a group; semi-groups describe sets possessing an associative binary operation (usually $+$) under which it is closed; Monoids are semigroups with an identity; and Groupoids are sets possessing a binary operation under which the set is closed. Monoids are Groupoids which (usually) are commutative.

Any two sets A and B, are such that their elements overlap $(A \cap B \neq \varnothing)$, or are disjoint $(A \cap B = \varnothing)$. The two sets are disjoint iff the properties of membership are mutually exclusive. The union of the two sets is not empty $(A \cup B \neq \varnothing)$, iff, at least one of the sets is non-empty, and $(A \cup B = \varnothing) \Leftrightarrow$ both A and B are empty sets. The difference of A and B, denoted $A \setminus B$, is the set formed by all elements of A, that are not elements of B. $A \setminus B$ can also be written $A - B$. When members of a set B, lie completely outside of another set A, we term those members the (relative) complement of A in B, $B \setminus A$, or the complement of B, relative to A. A similar concept is provided by the symmetric difference, $A + B$, or $A \Theta B$, or $A \nabla B$, described by the set of elements belonging to one, but not to two, of the indicated sets. This is also the union of the relative complements of A and B, $(B \setminus A) \cup (A \setminus B)$.

In a group G, such that elements $a, b, c \in \mathrm{G}$, the cancellation laws, which are an immediate consequence of the existence of inverse elements, are described via:

i/. If $a \circ b = a \circ c$, then $b = c$.

ii/. If $b \circ a = c \circ a$, then $b = c$.

Given a subgroup H of a group G, then for any element $x \in \mathrm{G}$, $\exists$ a left coset $x\mathrm{H}$, forming all of the elements xh, $h \in \mathrm{H}$. Right cosets are defined similarly, as $\exists$ a right coset $\mathrm{H}x$, with elements hx. The cosets of H in G are disjoint, and generate a partition of G. When H is a non-commutative group, then xH, and Hx, may be distinct. The set of aligned canonical objects formed as the cosets of H, are known as a transversal of the left/right cosets of H in G. Transversals generate precisely one member, q, of the transversal T, for which $x\mathrm{H} = q\mathrm{H}$. When $x\mathrm{H} = \mathrm{H}$, then H is denoted a normal subgroup. Normal subgroups are invariant under automorphisms, which are one-to-one correspondences known as isomorphisms, between 2 or more sets, possessing an identical domain and range, such as a permutation; the invariant automorphism is found to be the kernel of some structural property determining mapping, or homomorphism, preserving domain qualities in its range, such that

$$\theta(x * y) = \theta(x) \circ \theta(y). \tag{7}$$

Group homomorphisms satisfy the relationship

$$\theta(xy) = \theta(x)\theta(y). \tag{8}$$

A multiplicative function is thus necessarily homomorphic. In conjunction with isomorphisms, automorphisms, and homomorphisms, other morphisms, or mapping of sets, exist. These include, but are not limited to, epimorphisms, monomorphisms, and endomorphisms, which describe surjective or onto, injective or one-to-one or into, and homomorphic automorphic morphisms, respectively.

The set of elements of G which commute with every member of the group is termed the centre $\mathrm{Z(G)}$. The centre $\mathrm{Z(G)}$, is equal to the intersection of the subgroup $\mathrm{C}_a(x)$, known as the centralizer, consisting of all elements commuting with a particular element of a subgroup H of G. The centre of a group is a normal subgroup.

Just as the concept of sets is strengthened and refined by the requirements for admittance as a group. The concept of groups is more properly characterized through adherence to specific operations. The refinement begins with the definition of a ring R, satisfying:

Closure $(+, \times)$: R, is closed under the operations of addition and multiplication, satisfying each of the six properties:

1. Associative $(+)$: $\forall a,b,c \in R,\ a + (b + c) = (a + b) + c.$
2. Abelian $(+)$: $\forall a,b \in R,\ a + b = b + a.$
3. Identity $(+)$: $\exists\, 0 \in R:\ a + 0 = a,\ \forall a \in R.$

Here, 0 is a neutral element known as the zero element. Construction as a ring $\Rightarrow a.0 = 0, \ \forall a \in R.$

4. Inverse $(+)$: For each $a \in R, \ \exists -a \in R: \ a + (-a) = 0.$

5. Associative $(\times)$: $\forall a,b,c \in R, \ a(bc) = (ab)c.$

6. Distributive $\times(+), \ (+)\times$: $\forall a,b,c \in R, \ a(b+c) = ab + ac,$ and $(a+b)c = ac + bc.$

If the ring R, is commutative, then

7. Abelian $(\times)$: $\forall a,b \in R, \ ab = ba.$

And if it is a commutative ring with identity, then

8. Identity $(\times)$: $\exists 1 \, (\neq 0): \ a.1 = a, \ \forall a \in R.$

Where $\nexists$ any divisors of zero, (which occurs often in vector or matrix calculation), then we can define an integral domain.

9. Null Zero Division: $\forall a,b \in R, \ ab = 0$ only if $a = 0$ or $b = 0.$

A commutative ring is an integral domain precisely when the cancellation law holds in $(R, \times)$.

The concept of a field $\Leftrightarrow$

10. Group Inverses: For each $a \in R, \ a \neq 0, \ \exists a^{-1}: \ a^{-1}a = 1.$

Every field is an integral domain.

Examples of rings, denoted $\langle R, +, \times \rangle$ or $\langle R', \oplus, \otimes \rangle$ or $(R, +, \times)$ etc., include the set of even integers $(2\mathbb{Z},+)$, and the set of 2×2 real matrices $(\mathrm{M}_{2\times 2}, +, \times)$. A particularly relevant example of a ring is given by the set $\{0, 1, 2, \ldots, n-1\}$, under the operations of addition and multiplication modulo $n \in \mathbb{N}^0$, denoted $\mathbb{Z}_n$. The set of integers $\mathbb{Z}$, demonstrate an example of an integral domain, as does $(\mathbb{Z}_n, +, \times) = (\{0,1,2,\ldots,n-1\}, +, \times)$, for $n = p_i \in \mathbb{P}$. Fields include $\mathbb{Q}$, the set of rational numbers, $\mathbb{R}$, the set of real numbers, and $\mathbb{C}$, the set of complex numbers. The fields of primary use in this work is the set of integers modulo p_i, described by $\mathbb{Z}_{p_i} = (\{0,1,2,\ldots,p-1\}, +, \times), \ p_i \in \mathbb{P}$. A subset of a ring which is a ring satisfying the same operation as the larger ring, is termed a subring.

The ring properties delineated above can be augmented with further properties, such as possession of an identity, or unity (neutral element), describing a unitary ring. Similarly, a ring in which each non-zero element a, possesses an inverse element $aa^{-1} = e = a^{-1}a$, for (multiplicative) identity e, is a division ring. Any commutative division ring is a field. The division ring $\mathbb{H}$ of quaternions, describes a non-commutative division ring, and is thus, not a field.

Some rings are able to have other rings embedded within them. In this case, the larger ring is termed an over-ring. When an over-ring Q of another ring R possesses some non-zero regular elements b, such that $\forall a \in R,\ ab = 0$ or $ba = 0 \Leftrightarrow a = 0$, the elements are of the form ab^{-1} or $b^{-1}a$ (for a right and left quotient ring, respectively, or 2-sided normal quotient ring), and $\forall b \in R,\ b^{-1} \in Q$, then we call the ring a quotient/factor/residue class ring. A description of factor rings can also be provided via the concept of ideals. An ideal is a subring of a ring, which is closed under subtraction, and multiplication, by each of the ring elements. That is, $\forall a \in R,\ \forall x \in I:\ I$ is a subring of $R,\ ax, xa \in I$. Note that for non-communicative sets, only one of ax, and xa, may occur. ax is the left ideal, and xa is the right ideal. Otherwise, without qualification, the ideal is two-sided, and occasionally called a normal subring. An example of a subring is given by the set of multiples of any fixed integer in the ring of integers.

Using the concept of ideals, and cosets, a factor ring can be described as the ring R/K formed by the elements acting as cosets of an ideal K in the ring R. The cosets, called residue classes, are equivalence classes, where elements differ by a member of K. Thus the residue class is one of the equivalence classes that is a coset of an element of an ideal, or simply, any element of a factor ring. The operations of $(+,\times)$, or its equivalent $(+,.)$, on the set of residue classes modulo n, denoted $\mathbb{Z}_n$ satisfy requirement for a commutative ring with identity. When p is prime, then $\mathbb{Z}_{n=p}$ possesses no divisors of zero, and $\mathbb{Z}_p$ is a field. Any integral domain has a quotient ring that is a field, the field of fractions.

The sum and product of factor ring components are unique, and their coset sum or product, equal the sum or product of their individual cosets, respectively. If $uR = R$ for ring R, and $u \in R$, then u is termed a neutral element or unit. Units are multiplicatively invertible elements of a ring, integral domain, or other related structure. For example, the set of constant polynomials $\mathbb{P}(x)$ are units in a polynomial ring over a field. The counter-image of the zero of action of the factor ring image, (which possesses a unit element if R does), is termed the kernel.

Factor rings are a special case of factor spaces, or quotient spaces, which utilize set structure to impose a similar structure on the set of equivalence classes with respect to (wrt) a given equivalence relation. Thus, from the group properties: G/H of a group G by normal subgroup H, the set of cosets of H in G, is given by the factor/quotient group. Similarly, from the ring properties R/K of a ring R, by ideal K, the set of cosets of K in R, is given by the factor/quotient ring. Examples of refined factor/quotient spaces, include factor vector spaces, factor normal or Banach spaces, and factor Hilbert spaces. When a space S can be described in terms of a subspace T, and the factor space S/T, such that the 3 spaces possess the same property, it is said to possess the three-space property. Possession of an upper bound, or lower bound, would be such a property, termed a polyproperty.

Returning now to the concept of ideals, a left, right, or two-sided ideal, can be extended through its generation by a single element. Such a generation is termed a principal ideal. When the principal ideal satisfies requirements for an integral domain, the principal ideal integral domain is termed a principal ideal domain (PID). If every ideal in a ring is a principal ideal, then a principal ideal ring (PIR), similar to a PID, is generated.

In an integral domain $\mathrm{E}\setminus\{0\}$, there can exist a mapping g, termed a gauge, into the non-negative integers:

$$\forall a,b \in \mathrm{E}\setminus\{0\}, \quad g(ab) \geq g(a):$$

$$\text{for } b \in \mathrm{E} \text{ and } a \in \mathrm{E}\setminus\{0\},\ \exists q,r \in \mathrm{E}, \qquad (9)$$

$$\text{for which } b \in qa + r, \text{ and either } r = 0, \text{ or } g(r) < g(a).$$

When $g(a) = a \in \mathbb{Z}$, and a satisfies conventional addition and multiplication, then $b \in qa + r$ reduces to the division algorithm for integers. A gauge-bound division-algorithm-satisfying integral domain, is termed a Euclidean domain, or Euclidean ring. A Euclidean ring is a PID. An example of a Euclidean ring is the set of polynomials over any field, with the gauge being the degree of the polynomial.

The Gaussian field consisting of complex numbers $u + \mathrm{i}v$, $u,v \in \mathbb{Q}$, contains the algebraic integers in the Gaussian field, known as the Gaussian integers $a + \mathrm{i}b$, $a,b \in \mathbb{Z}$. The Gaussian integers are a Gaussian domain, or unique factorization domain. In a Gaussian domain, an integral domain provides representation of every non-zero non-unit, as a finite product of irreducible elements, in which the set of elements is unique. For example, in the Gaussian domain of Gaussian integers, $5 = (1 + 2\mathrm{i})(1 - 2\mathrm{i})$ is reducible, but 3 is irreducible, and hence prime, precisely because it is in a Euclidean domain.

Another refined group structure, is that of a module. A module is a commutative group M, satisfying left, or right, multiplication (termed exterior multiplication), or both, that is associative, distributive, and multiplies group elements by elements of a ring R, (called scalars), to generate group elements. M is then said to be a module over R, or an $R-$module. If, in addition, R is a unitary ring, and $i \circ g = g$ for ring identity i, and g any group element, then we term M a unitary $R-$module. An ideal in a ring R, is an $R-$module. Every commutative group is effectively a module over $\mathbb{Z}$, and every ring R can be viewed, as an $R-$module over itself. Submodules can exist as a module over a ring, within another module over the same ring, with the same addition. A condition, termed the ascending chain condition, ensures that no ascending chain of submodules $\mathrm{I}_1 \subseteq \mathrm{I}_2 \subseteq \ldots \subseteq \mathrm{I}_r$, each member of which is contained in the next, possesses more than a finite number of distinct members. This is equivalent to the maximum condition, ensuring that every non-empty set of submodules finitely generated by a finite number of elements, so also satisfying the finitely generated condition, possesses a maximal member. When a module satisfies the ascending chain condition, it is termed a Noetherian module. Being Noetherian is a $3-$space property. The set of integers $\mathbb{Z}$ form a Noetherian $\mathbb{Z}$-module, but the rationals $\mathbb{Q}$, do not.

Similarly, a condition termed the descending chain condition ensures that no descending chain of submodules $\mathrm{I}_1 \supseteq \mathrm{I}_2 \supseteq \ldots \supseteq \mathrm{I}_r$, contains more than a finite number of distinct members, so that for every chain, $\exists n : \mathrm{I}_n = \mathrm{I}_m \;\; \forall \, m \geq n$. This is equivalent to the minimum condition on a module, that every non-empty set of submodules possesses a minimal member. An Artinian module satisfies the descending chain condition. Every Artinian module is a Noetherian module, but the contra is not necessarily true. The integers $\mathbb{Z}$ are a Noetherian module, but not an Artinian $\mathbb{Z}$-module. The application of the maximum, and minimum, conditions, extends to groups, rings, and other related structures.

Mappings can be provided between one algebraic structure and another, whilst satisfying different conditions in the respective structure domains and images. When the structural properties of a domain are preserved in its image, such that operations $*$ in the domain, and $\circ$ in the range are satisfied, we term the mapping a homomorphism, described in Eqn. (7). In group theory, homomorphisms are surjective (onto), unless otherwise indicated. In a ring homomorphism, the mapping is between rings, such that

$$\forall x, y, \;\; \theta(x+y) = \theta(x) + \theta(y), \text{ and } \theta(xy) = \theta(x)\theta(y). \qquad (10)$$

In a module homomorphism, the mapping is between modules, such that for $\forall x, y \in$ an $R-$module, and $r \in$ the ring R,

$$\theta(x+y)=\theta(x)+\theta(y), \text{ and } \theta(rx)=r\theta(x). \qquad (11)$$

If R is a field, then θ is a linear mapping. The natural homomorphism or epimorphism, is the homomorphism υ from a group $\boldsymbol{G}$ to the factor group $\boldsymbol{G/K}$, that is defined, for rings and modules by its mapping to a left/right coset $\upsilon(x)=x+k$ or $\upsilon(x)=k'+x$, and for groups by $\upsilon(x)=xk$, or $\upsilon(x)=k'x$. Related epimorphisms exist for rings and modules w.r.t. ideals, and submodules, respectively.

APPENDIX

B: Module Mirror Primes (MMPs)

The set of natural numbers $\mathbb{N} = \{1, 2, 3, \ldots\}$ can be represented modulo 2, as the set $\{1, 2\}$ in row format as detailed in Table (a), or column format as detailed in Tables (b~c). The representations in Tables (a~c) support construction as the odd numbers $x \in \mathbb{N}$ taking values congruent to $1 \bmod 2$, and the even numbers taking values congruent to $0 \bmod 2$. The grey-shaded value 2, in Tables (a~c) indicate the only (even) prime.

Folded numbers (FNs)

The numerical layout of representations in Table (d), and Table (e), are examples of folded numbers FN(n)s, for $n \in \mathbb{N}$, where Table (d) describes the layout of the folded even number 4, FN(4), whilst Table (e) describes the layout of the folded odd number 5, FN(5). The choice for start row for the values $1, 2, \ldots,$ is arbitrary, but we will adopt the convention here, of beginning the sequence with the value 1 in the lower row. Note that subsequently, this may include an overhang in the upper row, as shown in Table (e).

(a)

1	2

(b)

2
1

(c)

1
2

(d)

3	2
1	2

(e)

5	4	3
	1	2

Note also that the representation of a FN is a construction of choice only, since for example, the odd number 7, can be written in column format in the manner of Table (f).

(f)

1	2
3	4
5	6
7	

In all that follows, any reference to a FN is described, for example, by the form of Table (g) for a folded even number 6, FN(6), and Table (h) for a folded odd number 13, FN(13).

(g)

6	5	4	3
	1	2	3

(h)

13	12	11	10	9	8	7
	1	2	3	4	5	6

Much of the work in this text, deals with the folded even number 30, represented in Table (i) below. The prime numbers contained in the set of natural numbers of FN(30), $\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29\}$, have been highlighted with a grey shaded background. In addition, the prime number 31 has been included, and will be dealt with shortly.

<u>Mirror-Primes (MPs), and Module Mirror Primes (MMPs)</u>

Note that some of the primes in each lower and upper row also coincide in columns. In Table (i), these are $\{7, 23\}$, $\{11, 19\}$, and $\{13, 17\}$. We shall term each pair of coincident primes, as a mirror-prime (MP) of $\mathrm{MP}(n)$, where $n \in \mathbb{N}$ is the value of the FN argument. If n is a module of the form $n = \prod_{i=1}^{r} p_i = p_1.p_2.\dots.p_i.\dots.p_r$, $p_i \in \mathbb{P}$, the set of primes in canonical ascendance, $p_1 = 2$, $p_2 = 3$, $p_3 = 5, \dots$ we term the MP as a module mirror prime (MMP) of n, $\mathrm{MMP}(n)$. . MMP measure structure details, which can be omitted on a first reading, are delineated in Appendix C. Since, $\prod_{i=1}^{3} p_i = 2.3.5 = 30$, then those primes are omitted from the presented list of primes shown in Table (i). The set of MMPs of $\{\mathrm{MMP}(30)\}$, is given by $\{\{7, 23\}, \{11, 19\}, \{13, 17\}\}$. Of special note are the pairs $\{1, 29\}$, and $\{*, 31\}$, both highlighted with a bold, large rectangle, the former of which may contain a prime, and the latter of which can appear as a prime, a MMP, or a MP, dependent upon the value of $n \in \mathbb{N}$. In addition, the odd squares 9, and 25, have been highlighted with a bold, small rectangle. Also, the twin primes $\{11,13\}$, $\{17,19\}$, and $\{29,31\}$, can be discerned. Note that the values in a FP expansion, above the value 1, and the asterisk shown, will always need to have their primality, or otherwise, verified.

(i)

31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15
*		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Some larger FNs which actually require representation as a (possibly lengthy) linear form, can be represented as stacked rows of a smaller FN. For example, the FN 210 of length 106 elements detailed in Table (j), FN(210), is represented as seven rows corresponding to the unfolded folded number 30, with the 7th row folded again, in half. Noting that the module $\prod_{i=1}^{4} p_i = 2.3.5.7 = 210$, primes greater than 7 are highlighted with a grey background, and squares by an emboldened small rectangle. MMPs of FN(210), such as $\{11,199\}$, are then represented as a full shaded column of two primes, between upper and lower emboldened lines. The set of MMPs of the FN and module 210, are indicated here as, MMP(210) = $\{\ \{11,199\},\ \{13,197\},\ \{17,193\},\ \{19,191\},\ \{29,181\},\ \{31,179\},\ \{37,173\},\ \{43,167\},\ \{47,163\},\ \{53,157\},\ \{59,151\},\ \{61,149\},\ \{71,139\},\ \{73,137\},\ \{79,131\},\ \{83,127\},\ \{97,113\},\ \{101,109\},\ \{103,107\}\ \}$. Note that the list of paired rows should ideally be viewed as being a single pair of rows.

(j)

210	209	208	207	206	205	204	203	202	201	200	199	198	197	196	195	194	193	192	191	190	189	188	187	186	185	184	183	182	181
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
180	179	178	177	176	175	174	173	172	171	170	169	168	167	166	165	164	163	162	161	160	159	158	157	156	155	154	153	152	151
30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59
150	149	148	147	146	145	144	143	142	141	140	139	138	137	136	135	134	133	132	131	130	129	128	127	126	125	124	123	122	121
60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89
120	119	118	117	116	115	114	113	112	111	110	109	108	107	106	105														
90	91	92	93	94	95	96	97	98	99	100	101	102	103	104	105														

A representation of the first 300 row pairs of FN(2310) in Table (k), corresponding to the module $\prod_{i=1}^{5} p_i = 2.3.5.7.11 = 2310$, is detailed below, excluding the primes $\{2,3,5,7,11\}$. In the table, primes greater than 11 are again highlighted with a grey background, squares by a small bold rectangle, and MMPs of FN(2310), such as $\{17, 2293\}$, are represented as a shaded column of two primes, between upper and lower emboldened lines.

(k)

2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
3	3	3	3	3	3	3	3	3	3	3	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
1	0	0	0	0	0	0	0	0	0	0	9	9	9	9	9	9	9	9	9	9	8	8	8	8	8	8	8	8	8
0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1
										1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2
	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
8	7	7	7	7	7	7	7	7	7	7	6	6	6	6	6	6	6	6	6	6	5	5	5	5	5	5	5	5	5
0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1
3	3	3	3	3	3	3	3	3	3	4	4	4	4	4	4	4	4	4	4	5	5	5	5	5	5	5	5	5	5
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
5	4	4	4	4	4	4	4	4	4	4	3	3	3	3	3	3	3	3	3	3	2	2	2	2	2	2	2	2	2
0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1
6	6	6	6	6	6	6	6	6	6	7	7	7	7	7	7	7	7	7	7	8	8	8	8	8	8	8	8	8	8
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1
2	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	9	9	9	9	9	9	9	9	9
0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1
										1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
9	9	9	9	9	9	9	9	9	9	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
9	8	8	8	8	8	8	8	8	8	8	7	7	7	7	7	7	7	7	7	7	6	6	6	6	6	6	6	6	6
0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	4	4	4	4	4	4	4	4	4	4
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
6	5	5	5	5	5	5	5	5	5	5	4	4	4	4	4	4	4	4	4	4	3	3	3	3	3	3	3	3	3
0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
5	5	5	5	5	5	5	5	5	5	6	6	6	6	6	6	6	6	6	6	7	7	7	7	7	7	7	7	7	7
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
3	2	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0
0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2
8	8	8	8	8	8	8	8	8	8	9	9	9	9	9	9	9	9	9	9	0	0	0	0	0	0	0	0	0	0
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	9	9	9	9	9	9	9	9	9	9	8	8	8	8	8	8	8	8	8	8	7	7	7	7	7	7	7	7	7
0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1
2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9

2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	6	6	6	6	6	6	6	6	6	6	5	5	5	5	5	5	5	5	5	5	4	4	4	4	4	4	4	4	4
0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1
2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
4	4	4	4	4	4	4	4	4	4	5	5	5	5	5	5	5	5	5	5	6	6	6	6	6	6	6	6	6	6
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	3	3	3	3	3	3	3	3	3	3	2	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1
0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1	0	9	8	7	6	5	4	3	2	1
2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
7	7	7	7	7	7	7	7	7	7	8	8	8	8	8	8	8	8	8	8	9	9	9	9	9	9	9	9	9	9
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
2	.	.	.																										
0																													
1																													
0																													
3	.	.	.																										
0																													
0																													

Table (1) utilizes the $30-\text{column}$ stacking of rows of length 210, to portray the collection of twin primes, such as $(11,13)$, found in the set of natural numbers $1,2,\ldots,2309,\ 2310$, with the exclusion of the twin primes $(3,5)$, and $(5,7)$. Note the inclusion of the square 169, indicated by a small bold rectangle, in the grey-shaded pair $(167,169)$, and the related grey-shaded twin prime-pair $(1427,1429)$, situated in the same stack column. The inclusion demonstrates that prime numbers and prime-pairs can be related to smaller squares, as well as other smaller primes, in the same stack column.

(1)

11 13	17 19	29 31	41 43	59 61	71 73	101 103	107 109	137 139	149 151	167 169	179 181	191 193	197 199	
	227 229	239 241		269 271	281 283	311 313		347 349						419 421
431 433			461 463			521 523			569 571		599 601		617 619	
641 643		659 661												
											809 811	821 823	827 829	
	857 859		881 883								1019 1021	1031 1033		1049 1051
1061 1063			1091 1093			1151 1153								
											1229 1231			
	1277 1279	1289 1291	1301 1303	1319 1321										
										1427 1429		1451 1453		
1481 1483	1487 1489							1607 1609	1619 1621				1667 1669	
	1697 1699		1721 1723				1787 1789					1871 1873	1877 1879	
			1931 1933	1949 1951			1997 1999	2027 2029				2081 2083	2087 2089	
2111 2113		2129 2131	2141 2143					2237 2239						
										2267 2269				2309 2311

APPENDIX

C: Module Mirror Prime (MMP) Structure

Considering any module of length $\prod_{i=1}^{r} p_i = p_1 . p_2 . \dots . p_r$, which we write as $\prod_{1\sim r} p_r$, or simply Πp_r, 5 integer value positions of particular relevance are:

a). $\Pi p_r = p_1 . p_2 . \dots . p_r$; the maximum length of each module.

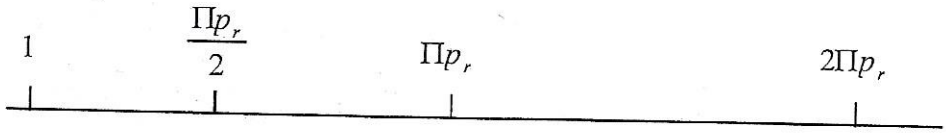
b). $n\Pi p_r, n = p_{r+1}$; the maximum length of n modules of type (a).

c). $n\Pi p_r + 1, \ n = \{0, 1, 2, \dots, p_{r+1}\}$; the start value of each of the n modules.

d). $\left\lceil\sqrt{\Pi p_r}\right\rceil^{PI}$; the smallest prime number greater than $\sqrt{\Pi p_r}$. This is the largest prime number required to have its multiples removed from the module(s), up to the value of its square, $\left(\left\lceil\sqrt{\Pi p_r}\right\rceil^{PI}\right)^2$. This is necessarily inclusive of the module maximum value Πp_r, but less than twice the maximum module value $2\Pi p_r$.

e). $\left(\left\lceil\sqrt{\Pi p_r}\right\rceil^{PI}\right)^2$; the largest value able to be included as removed from the list of generated primes, via removal of the multiples of each prime $p_j = 2, 3, 5, \dots, p_k$ such that $p_j \le p_k = \left\lceil\sqrt{\Pi p_r}\right\rceil^{PI}$.

Aligning some of these fundamental values along a standard, positive number line, delivers the alignment of integer values:



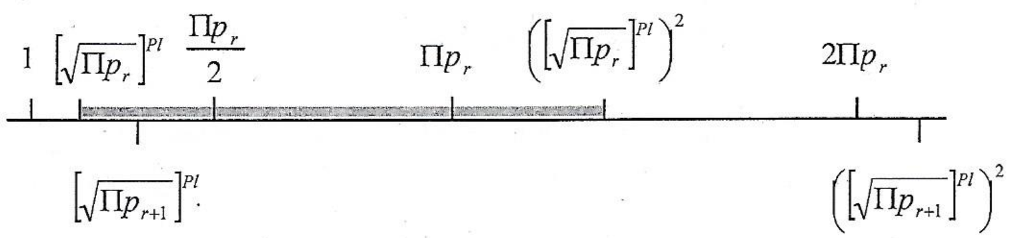
Then considering the three values $\frac{\Pi p_r}{2}$, $\left\lceil\sqrt{\Pi p_r}\right\rceil^{PI}$, and $\left\lceil\sqrt{\Pi p_{r+1}}\right\rceil^{PI}$, we can note immediately that $\left\lceil\sqrt{\Pi p_r}\right\rceil^{PI} < \left\lceil\sqrt{\Pi p_{r+1}}\right\rceil^{PI}$, placing the former to the left of the latter on the number line. Now considering $\frac{\Pi p_r}{2} > \left\lceil\sqrt{\Pi p_{r+1}}\right\rceil^{PI}$, this is true precisely when $\frac{\sqrt{\Pi p_r}}{2}\sqrt{\Pi p_r} > \left\lceil\sqrt{\Pi p_{r+1}}\right\rceil^{PI}$, which implies when $\frac{\sqrt{\Pi p_r}}{2}$ is larger than $\left\lceil\sqrt{p_{r+1}}\right\rceil$. Using

Bertrand's postulate established by Chebyshev [1], where p_{r+1} is a maximum value, then $\exists p : n < p < 2n-2 \;\Rightarrow\; p_r < p_{r+1} < 2p_r - 2$. But for the p_{r+1}th prime, this means that $p_{r+1} < p_r + (2p_r - 2) = 3p_r - 2$. Since $\frac{\Pi p_r}{4} > 3p_r - 2$, for $r > 3$, then we can conclude that $\frac{\Pi p_r}{2} > \left[\sqrt{\Pi p_{r+1}}\right]^{PI}$, $r > 3$.

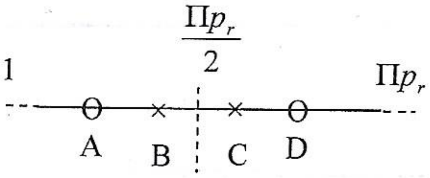
In addition, noting that for some positive integer $\alpha \in \mathbb{Z}^+$, $\alpha < \Pi p_r$, we have

$(\Pi p_r + \alpha) < 2\Pi p_r \quad \Rightarrow \quad \left(\sqrt{\Pi p_r + \alpha}\right)^2 < 2\Pi p_r \quad \Rightarrow \left(\left[\sqrt{\Pi p_r}\right]^{PI}\right)^2 < 2\Pi p_r$, then $\left(\left[\sqrt{\Pi p_r}\right]^{PI}\right)^2$ lies between Πp_r and $2\Pi p_r$ on a standard number line.

Finally, from $\left(\left[\sqrt{\Pi p_{r+1}}\right]^{PI}\right)^2$, we have $\left(\left[\sqrt{\Pi p_{r+1}}\right]^{PI}\right)^2 = \left(\sqrt{\Pi p_{r+1} + \alpha}\right)^2$, and expanding the right-hand side, $\Rightarrow \left(\sqrt{\Pi p_{r+1} + \alpha}\right)^2 = \Pi p_{r+1} + \beta,\ \beta \in \mathbb{Z}^+$. Since $p_{r+1} > 2$, then we can deduce that $\left(\left[\sqrt{\Pi p_{r+1}}\right]^{PI}\right)^2$ is on the right-hand side of $2\Pi p_r$ on a standard number line. Including the derived values and their relationships onto the number line previously shown, we have



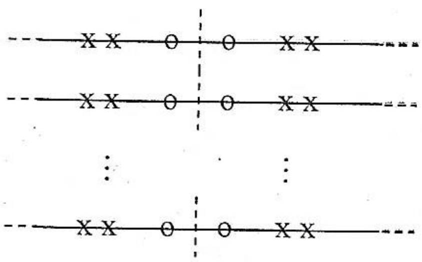
The grey shaded linear region indicates the stretch of values $\left]\left[\sqrt{\Pi p_r}\right]^{PI}, \left(\left[\sqrt{\Pi p_r}\right]^{PI}\right)^2\right[$, within which all primes and prime pairs able to be removed, are present. The removed factors, kp_i, $i \le r$, $k \in \mathbb{Z}^+$, are symmetric, wrt the initial module $[1, \Pi p_r]$, about the values $\frac{\Pi p_r}{2}$: $\mathrm{A} + \mathrm{D} = \mathrm{B} + \mathrm{C} = \Pi p_r$, and $\Pi p_r - \mathrm{A} + \Pi p_r - \mathrm{D} = \Pi p_r = \Pi p_r - \mathrm{B} + \Pi p_r - \mathrm{C}$. The pairs (A, D), and (B, C), form Mirror Factors (MFs) (Section 1) of the FN, $\mathrm{FN}(\Pi p_r)$ (Appendix B).



Now relating concatenated lengths of the intervals $[1, \Pi p_r]$, and stacking the lengths $[1, \Pi p_r]$ below each other in the form:

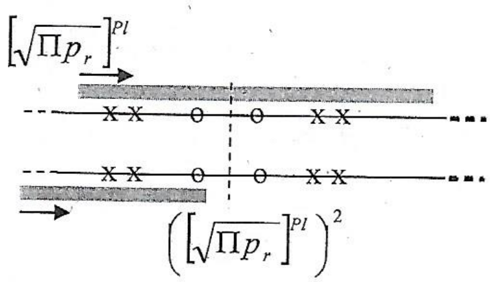
$$\begin{gathered}[\Pi p_r + 1,\ 2\Pi p_r]\\ [2\Pi p_r + 1,\ 3\Pi p_r]\\ \vdots \quad , \quad \vdots\\ [n\Pi p_r + 1,\ (n+1)\Pi p_r]\\ \vdots \quad , \quad \vdots\\ [p_{r+1}\Pi p_r + 1,\ (p_{r+1}+1)\Pi p_r],\end{gathered}$$

We can envisage that any prime, or prime pair appearing as undeleted in the list $[1, \Pi p_r]$, will also be available in some of the list of intervals below it, in the manner shown below, for prime pairs $(\mathrm{x},\mathrm{x}) = (p_i, p_j) \in \mathbb{P}\times\mathbb{P}$, $(p_j = p_i + 2)$ and single primes $(\mathrm{o}) = (p_i) \in \mathbb{P}$:

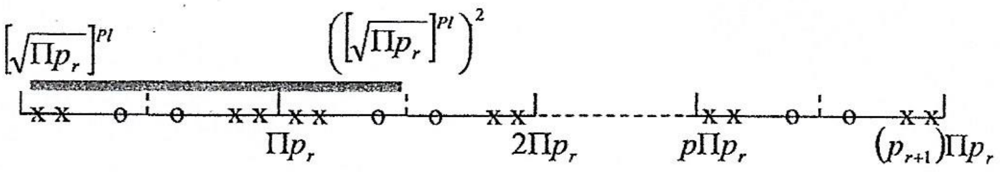


Until such time as the appropriate primes and multiples of primes have been deleted.

The number-line analysis shown earlier indicates there will be a region in the first two (rows of) modules in which any undeleted number is prime



corresponding to the p_{r+1} concatenated modules of length Πp_r :



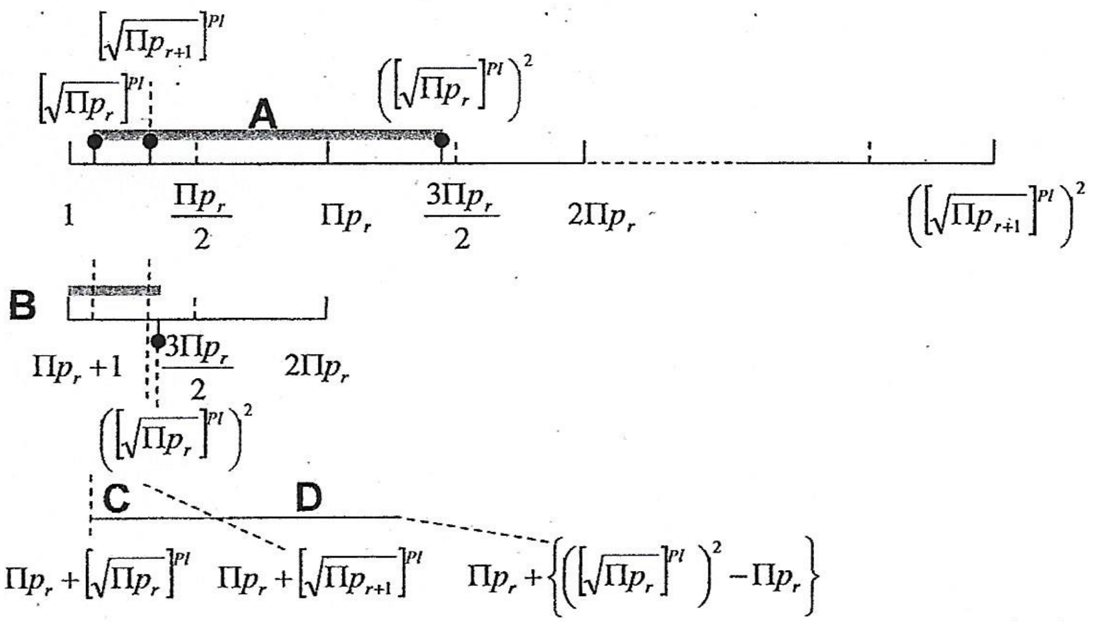
We can now note that in the second module, the region highlighted grey, represents the ascending values in the interval of length $\left(\left[\sqrt{\Pi p_r}\right]^{PI}\right)^2 - \Pi p_r$, given by $\left[(\Pi p_r + 1), \left(\left[\sqrt{\Pi p_r}\right]^{PI}\right)^2\right]$. Appealing to Bertrand's postulate again, (or otherwise), we can argue that for some value $\varepsilon \le \frac{\Pi p_r}{2}$, $\forall \Pi p_r : p_r > 2$, we will always have

$$\left(\sqrt{\Pi p_r + \varepsilon}\right)^2 \le \left(\sqrt{\Pi p_r + \frac{\Pi p_r}{2}}\right)^2 = \frac{3\Pi p_r}{2},$$

$$\Rightarrow \qquad \left(\left[\sqrt{\Pi p_r}\right]^{PI}\right)^2 \le \frac{3\Pi p_r}{2},$$

$$\Rightarrow \qquad \left(\left[\sqrt{\Pi p_r}\right]^{PI}\right)^2 - \Pi p_r \le \frac{\Pi p_r}{2}.$$

Hence the list of non-deleted primes in the second-row module is certainly greater than $\sqrt{\Pi p_{r+1}}$, by line 25, and from above, is less than $\frac{3\Pi p_r}{2}$, so on the LHS of $\frac{3\Pi p_r}{2}$.



Including these bounds into the first and second row module number-lines, describes the relationship indicated in the figure above, which is true for all modules Πp_r :

On these number-lines, we have the regions:

A). From 1 to $\left(\left[\sqrt{\Pi p_{r+1}}\right]^{PI}\right)^2$, with the grey shaded area $\left[\left[\sqrt{\Pi p_r}\right]^{PI}, \left(\left[\sqrt{\Pi p_r}\right]^{PI}\right)^2\right]$, which is less than $2\Pi p_r$. It comprising the non-deleted primes contained in the intervals $]1, \Pi p_r]$ and $\left[\Pi p_r + 1, \left(\left[\sqrt{\Pi p_r}\right]^{PI}\right)^2\right[$.

B). The number-line of length $2\Pi p_r - (\Pi p_r + 1)$, containing the grey shaded area of length $\left(\left[\sqrt{\Pi p_r}\right]^{PI}\right)^2 - \Pi p_r$ in the second row module. This is the interval $\left[\Pi p_r + 1, \left(\left[\sqrt{\Pi p_r}\right]^{PI}\right)^2\right[$, containing the non-deleted primes in the number-line values greater than Πp_r corresponding to the positions

$$\Pi p_r + 1 < \Pi p_r + \left[\sqrt{\Pi p_r}\right]^{PI} < \Pi p_r + \left[\sqrt{\Pi p_{r+1}}\right]^{PI} < \left(\left[\sqrt{\Pi p_r}\right]^{PI}\right)^2 .$$

C). The region $\left[\Pi p_r + \left[\sqrt{\Pi p_r}\right]^{PI}, \Pi p_r + \left[\sqrt{\Pi p_{r+1}}\right]^{PI} - 1\right]$, which coincides with the first row module values $\geq \left[\sqrt{\Pi p_r}\right]^{PI}$, but less than $\left[\sqrt{\Pi p_{r+1}}\right]^{PI}$. This means that any non-deleted prime-pairs within the region $\left[\Pi p_r + 1, \left[\sqrt{\Pi p_{r+1}}\right]^{PI} - 1\right]$ in the first row module, will also appear in the second row module, but will not be guaranteed to appear in any larger row position modules.

D). The non-deleted prime, and prime-pair list in the interval $\left[\left[\sqrt{\Pi p_{r+1}}\right]^{PI}, \left(\left[\sqrt{\Pi p_r}\right]^{PI}\right)^2\right]$ of the first row module region coinciding with the interval $\left[\Pi p_r + \left[\sqrt{\Pi p_{r+1}}\right]^{PI}, \left(\left[\sqrt{\Pi p_{r+1}}\right]^{PI}\right)^2\right]$ of the second row module, of length $\left(\left(\left[\sqrt{\Pi p_{r+1}}\right]^{PI}\right)^2 - \Pi p_r - \left[\sqrt{\Pi p_{r+1}}\right]^{PI} + 1\right)$.

Some primes, prime-pairs, and squares appearing in the corresponding region in the first row module, will also, necessarily, provide the potential for other, larger primes, to appear in the same positions in subsequent row modules. Subsequently, by Bertrands theorem (line 23) or otherwise, for some prime or square in the respective first row module region, there must be generated a prime in at least one of the next p modules of the larger set of modules of length $p_{r+1}\Pi p_r$. Note that the same cannot be said of the generation of a twin prime (TP). Referring now to the bounds

$$\left[\sqrt{\Pi p_r}\right]^{PI} < \left[\sqrt{\Pi p_{r+1}}\right]^{PI} < \frac{\Pi p_r}{2} < \Pi p_r < \left(\left[\sqrt{\Pi p_r}\right]^{PI}\right)^2 < \frac{3\Pi p_r}{2} < \left(\left[\sqrt{\Pi p_{r+1}}\right]^{PI}\right)^2,$$

as we move from one bound to the next, LHS to RHS, every bound increases in value faster than the bound preceding it. This means that as the value of p_r increases, the distance between the bounds increases faster towards each RH bound; so each interval in the list of bounds above, increases faster than the interval before it.

If we can demonstrate that a TP $(p_i, p_i + 2)$ is always generated in each module, then we can prove that $\exists$ an infinite number of TPs. However, it may be the case that a class of TPs evolve via two distinct primes $p_u, p_v : p_u \neq p_v \pm 2$.

APPENDIX

D: Prime Modules of Modules of 30 Units $(M_{p_i \times 30})$

The following figure demonstrates the construction of the prime modules p_i, denoted module_{p_i}, of modules of 30 units, module_{30}, each bounded by the upper rectangle in columns (d) ~ p_7, dealt with in Section 5, page 28, (g) ~ p_{11}, (i) ~ p_{13}, (j) ~ p_{17}, (k) ~ p_{19}, (l) ~ p_{23}, (m) ~ p_{29}, (n) ~ p_{31}, each with their default Twin Prime Indicator (TPI) states, (Section 5, page 25), in the column to the left of the column of modules p_i, and their modified TPI intersection states in the column to the right of the column of modules p_i.

The square of each value p_i in the module_{p_i}, is indicated in its module_{30} form, by a small, bold, rectangle around the corresponding value. Note that in column (n), the square value in row 33 is intended to indicate that it lies outside of the first module, and is a repeat of the value $(3)1$ in column two. In each module_{p_i} of modules_{30}, denoted $M_{p_i \times 30}$, the 30 partitioned values $\{2,3,\ldots,30,(3)1\}$ are indicated, with the final value in each $M_{p_i \times 30}$, being 30. The two non-TPI primes 7, and 23, highlighted as shaded dark-grey squares, and the six TPI-related primes $\{(11,13),(17,19),(29,(3)1)\}$, are highlighted as shaded light-grey squares.

The column of unmodified TPIs in column (c), are all in precisely the same state, with only the primes 2, 3, and 5 removed, and are thus each of the form of the module of 30 units described in Section 2, page 14, excluding $M_{7\times 30}$. Each column of modified TPIs to the LHS of each column module is comprised of the concatenation of the modifications made to the first p_i rows of the module_{p_i}. Correspondingly, excluding $M_{7\times 30}$, which includes column (e) of modified TPIs, a concatenation of the first 7 modified TPIs in row 1 to row 7, each subsequent column of TPIs in the column to the RHS of each module_{p_i}, is generated through use of the operation of intersection of TPI states. For example, column (h) to the right of module_{11}, in column (g) is formed via column (h) TPIs = (column (e) TPIs ∩ column (f) TPIs).

Every column module, excluding module_7, display their repeated p_i – division modified TPIs_{30}, to the immediate left of the respective modules, and the module-intersection modified TPIs_{30}, to the immediate right of the respective modules.

a.	b.	c.	d.					g.			i.			j.		k.		l.		m.		n.
1	1	—	7	14	21	28		11	22		13	26		17		19		23		29		
2	31	—	5	12	19	26		3	14	25	9	22		4	21	8	27	16		28		(3)1
3	61	—	3	10	17	24		6	17	28	5	18		8	25	16		9		27		2
4	91	—	(3)1	8	15	22	29	9	20		(3)1	14	27	12	29	5	24	2	25	26		3
5	121	—	6	13	20	27		(3)1	12	23	10	23		16		13		18		25		4
6	151	—	4	11	18	25		4	15	26	6	19		3	20	2	21	11		24		5
7	181	—	2	9	16	23	30	7	18	29	2	15	28	7	24	10	29	4	27	23		6
8	211	—						10	21		11	24		11	28	18		20		22		7
9	241	—						2	13	24	7	20		15		7	26	13		21		8
10	271	—						5	16	27	3	16	29	2	19	15		6	29	20		9
11	301	—						8	19	30	12	25		6	23	4	23	22		19		10
12	331	—									8	21		10	27	12		15		18		11
13	361	—									4	17	30	14		(3)1	20	8		17		12
14	391	—												(3)1	18	9	28	(3)1	24	16		13
15	421	—												5	22	17		17		15		14
16	451	—												9	26	6	25	10		14		15
17	481	—												13	30	14		3	26	13		16
18	511	—														3	22	19		12		17
19	541	—														11	30	12		11		18
20	571	—																5	28	10		19
21	601	—																21		9		20
22	631	—																14		8		21
23	661	—																7	30	7		22
24	691	—																		6		23
25	721	—																		5		24
26	751	—																		4		25
27	781	—																		3		26
28	811	—																		2		27
29	841	—																		(3)1	30	28
30	871	—																				29
31	901	—																				30
32	931	—																				
33	961	—																				(3)1
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...