

The Structure of Primes and Prime Lattice Theory

Simon Mark Horvat

This paper derives the structure of Prime numbers from First Principles and explains how the structure causes the Prime Number Theorem. Factorisation algorithms are derived and a Prime Number Generator investigated.

Every problem contains within itself the seeds of its own solution.--Stanley Arnold

Discussion

Complexity Theory has shown that simple systems, when combined, can have complex consequences. This is the case with Prime numbers. For thousands of years Prime numbers have tantalised mathematicians with their possible hidden structure. In some respects they appear structured, (*Riemann's Hypothesis, Prime Sums*), in others they so lack a structure that we question whether they aren't some form of randomness (*Prime Counting Function, Prime Gap*).

While reading a biography of Paul Erdos [Hoffman 1998 (1)] I was inspired to work through Euclid's Proof of the Infinitude of Primes [Hoffman 1998 (2)] and realised that the Proof could be generalised in a number of ways. Investigating these General Forms I found an equation which appeared to be a Prime Number Pair Generator. Further General Forms produced Composites as well as Primes and acted as a Factorisation equation. While trying to understand why some General Forms also generated Composites I discovered the structure of Prime numbers. Refer to Section 6 of this paper for the details of these Generalisations

In Section 1, I show that Prime numbers are structured, and form the starting points of Composite strands in a Lattice-like structure of Composite numbers over the Integers, \mathbb{Z} . I show how this structure may be derived from First Principles and formally describe this structure in the

Fundamental Theorem of Primes:

All Integers are members of only one of the sets:

- Prime Base, $\mathbf{B} = \{\pm P_1, \pm P_2\} = \{-3, -2, 2, 3\}$
- Subtractive Primes, \mathbf{P}_S , of the form $2.3.n - 1$, $n \in \mathbb{Z}$
- Additive Primes, \mathbf{P}_A , of the form $2.3.n + 1$, $n \in \mathbb{Z}$
- Composites of the forms $2.n, 3.n$, $n \in \mathbb{Z}$, $|n| \neq 1$, ie Multiples of 2 and/or 3, includes 0
- Composites, of the form $2.3.n \pm 1$, $n \in \mathbb{Z}$, ie Multiples of Primes other than 2 or 3

Subsequent sections, explain why the Prime Number Theorem holds, derive Factorisation algorithms from the Prime structure, demonstrate multiplication relationships, extend the Prime structure into other domains, detail the research into a Prime Number Generator which lead me to discover the Prime Structure, and examine Symmetric Prime Lattices.

As per common practice, [Ingham, 1932] and [Jameson, 2003], "1" will be considered as neither Prime nor Composite.

I will use both Product, Π , and Primorial, $P_i\#$, notation in equations, where $P_n\# = \prod_{i=1}^n P_i$, such that (st) P_i is the i^{th} positive Prime, $P_1=2, P_2=3, P_3=5, P_4=7, \dots$

Section 1: Structure of Primes over \mathbb{Z}

Definition: Prime Number

Let $P \in \mathbb{Z}$. We say that P is Prime if its only (+)ve divisors are 1 and $|P|$

Theorem 1: Euclid's Theorem of the Infinitude of Primes:

There are an infinite number of Primes

From Euclid's Proof of the Infinitude of Primes, *cf Appendix A*, we know that the equation

$$Q = \prod_{i=1}^n P_i \pm 1$$

can be used to prove that there are an infinite number of Primes. This paper demonstrates how the structure of Prime Numbers can be derived from this equation.

Theorem 2: Fundamental Theorem of Arithmetic

Any positive integer can be expressed uniquely as a product of primes, ignoring ordering of prime factors within the expression.

This theorem is also known as the Unique Factorization Theorem. [Hardy and Wright 1979]
[Weisstein (1)]

Theorem 3: Odd Primes

All prime numbers $\pm P_i$, other than ± 2 , are odd, ie are of the form $\pm P_i = 2.n \pm 1$, $n \in \mathbb{Z}$

Proof:

For $n \in \mathbb{Z}$

The Prime number 11 may be expressed in the form $P_i = 2.n \pm 1$, $n=5$ or 6

The Prime number 61 may be expressed in the form $P_i = 2.n \pm 1$, $n=30$ or 31

The Prime number -11 may be expressed in the form $-P_i = 2.n \pm 1$, $n=-5$ or -6

The Prime number -61 may be expressed in the form $-P_i = 2.n \pm 1$, $n=-30$ or -31

Therefore there exist Primes of the form $\pm P_i = 2.n \pm 1$

From modulo arithmetic we know that all integers can be expressed in the form $z = 2n \pm r$, where $r=0, 1$

$z = 2n \pm 0 = 2n$ is even, ie divisible by two, thus either $z = \pm 2$ or z is a multiple of 2

$z = 2.n \pm 1$ is odd, ie is not divisible by 2

All prime numbers $\pm P_i$, other than $\pm P_2$, are indivisible by 2 or they would be Composite with a factor of 2 and therefore not Prime

Therefore all Prime Numbers, other than ± 2 , are of the form $\pm P_i = 2.n \pm 1$, $n \in \mathbb{Z}$

While it can be shown that all Primes, other than 3, are of the form $\pm P_i = 3.n \pm 1$, n is even for every Prime other than $\pm P_1 = \pm 2$, the case when $n = \pm 1$. It can be argued that such a theorem is implicitly about $2 \times 3 = P_2 \#$

Theorem 4: Additive and Subtractive Prime sets

All prime numbers $\pm P_i$, other than ± 2 and ± 3 , are of the form $\pm P_i = (2.3.n) \pm 1 = n.P_2 \# \pm 1$,

$n \in \mathbb{Z}$. $\pm P_i = n.P_2 \# - 1$ are termed Subtractive Primes, $\pm P_i = n.P_2 \# + 1$ are Additive Primes

Proof:

For $n \in \mathbb{Z}$

The Primes 5 and 47 are of the form $n.P_2\# - 1$, $n=1$ and 8 respectively
 The Primes 7 and 37 are of the form $n.P_2\# + 1$, $n=1$ and 6 respectively
 The Primes -5 and -47 are of the form $n.P_2\# + 1$, $n=-1$ and -8 respectively
 The Primes -7 and -37 are of the form $n.P_2\# - 1$, $n=-1$ and -6 respectively
 Therefore there exist Primes of the forms, $\pm P_i = n.P_2\# \pm 1$, $n \in \mathbb{Z}$

From modulo arithmetic we know that all integers can be expressed in the form $z=(6.n) \pm r$, where $r=0, 1, 2, 3$

If $r=0$, then $z=6n = (2.3.n)$ and is divisible by both ± 2 and ± 3
 If $r=2$, then $z=6n \pm 2 = 2.(3.n \pm 1)$ and is divisible by ± 2 . If $n=0$, $r=2$, then $z=\pm 2$
 If $r=3$, then $z=6n \pm 3 = 3.(2.n \pm 1)$ and is divisible by ± 3 . If $n=0$, $r=3$, then $z=\pm 3$

If $r=1$, then $z=6n \pm 1 = (2.3.n) \pm 1$ and is indivisible by both 2 and 3
 All prime numbers $\pm P_i$, other than $\pm P_1$ and $\pm P_2$, are indivisible by both ± 2 and ± 3

Therefore all prime numbers, other than ± 2 and ± 3 , are of the form $\pm P_i=(2.3.n) \pm 1$, $n \in \mathbb{Z}$

Theorem 4 may be extended to address all Primes

Theorem 5: Prime Real Form

All Prime numbers are Integers of the form $\pm P_i = (2.3.r) \pm 1 = r.P_2\# \pm 1$, $r \in \mathbb{R}$

Proof:

For all Prime Integers other than ± 2 or ± 3 refer to the Theorem of Additive and Subtractive Prime sets. For these Primes, r is restricted to integer values, $r=n \in \mathbb{Z}$

$$\text{For } \pm P_0 = \pm 1, r = \frac{\pm 1}{3}, \text{ or } r = 0$$

$$\text{For } \pm P_1 = \pm 2, r = \frac{\pm 1}{2}, \text{ or } r = \frac{\pm 1}{2.3}$$

$$\text{For } \pm P_2 = \pm 3, r = \frac{\pm 1}{3}, \text{ or } r = \frac{\pm 2}{3}$$

Therefore, all Prime numbers are Integers of the form $\pm P_i = (2.3.r) \pm 1 = r.P_2\# \pm 1$, $r \in \mathbb{R}$

Theorem 6:

There exist prime numbers $\pm P_i$, other than ± 2 , ± 3 and ± 5 , which are not of the form $\pm P_i=(n.P_3\#) \pm 1$, $n \in \mathbb{Z}$

Proof:

From modulo arithmetic we know that all integers can be expressed in the form $z=(30.n) \pm r$, where $r=0, 1, 2, \dots, 15$, $n \in \mathbb{Z}$

The Primes 23 and 173 are of the form $(n.P_3\#) - 7$, $n=1$ and 6 respectively
 The Primes 41 and 251 are of the form $(n.P_3\#) + 11$, $n=1$ and 8 respectively
 The Primes -23 and -173 are of the form $-(n.P_3\#) + 7$, $n=1$ and 6 respectively
 The Primes -41 and -251 are of the form $-(n.P_3\#) - 11$, $n=1$ and 8 respectively

Therefore there exist Primes, other than ± 2 , ± 3 and ± 5 , which are not of the form

$$\pm P_i = (n \cdot P_3 \#) \pm 1, \quad n \in \mathbb{Z}$$

What is the significance of the different outcomes when comparing Theorems 4 and 6 ?

The first 5 negative, and the first 32 positive, Primes in standard representation

-7, -5, -3, -2, -1, 1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127

The sample of Primes extended and expressed in light of Theorem 4 in a Modulo 6 grid representation.

$3(2n-1)$	$2(3n-1)$	$6n-1$	$6n$	$6n+1$	$2(3n+1)$	$3(2n+1)$
...
...	...	-5x5	$-(2 \times 3) \times 4$	-23
...	...	-19	$-(2 \times 3) \times 3$	-17
-3x5	-2x7	-13	$-(2 \times 3) \times 2$	-11	-2x5	...
-3x3	-2x4	-7	$-(2 \times 3)$	-5	-2x2	...
-3	-2	-1	0	1	2	3
	2x2	5	2x3	7	2x4	3x3
	2x5	11	$2 \times 3 \times 2$	13	2x7	3x5
	...	17	$2 \times 3 \times 3$	19
	...	23	$2 \times 3 \times 4$	5x5
		29	$2 \times 3 \times 5$	31		
		5x7	$2 \times 3 \times 6$	37		
		41	$2 \times 3 \times 7$	43		
		47	$2 \times 3 \times 8$	7x7		
		53	$2 \times 3 \times 9$	5x11		
		59	$2 \times 3 \times 10$	61		
		5x13	$2 \times 3 \times 11$	67		
		71	$2 \times 3 \times 12$	73		
		7x11	$2 \times 3 \times 13$	79		
		83	$2 \times 3 \times 14$	5x17		
		89	$2 \times 3 \times 15$	7x13		
		5x19	$2 \times 3 \times 16$	97		
		101	$2 \times 3 \times 17$	103		
		107	$2 \times 3 \times 18$	109		
		113	$2 \times 3 \times 19$	5x23		
		7x17	$2 \times 3 \times 20$	11x11		
		5x5x5	$2 \times 3 \times 21$	127		
			
		173	$2 \times 3 \times 29$	5x5x7		
			
		13x29	$2 \times 3 \times 63$	379		
		383	$2 \times 3 \times 64$	5x7x11		
		389	$2 \times 3 \times 65$	17x23		
			

Table 1-1: "Integers modulo 6"

This gives a new way of looking at Theorem 4, using the Fundamental Theorem of Arithmetic.

There is a Lattice-like structure of Composite strands over \mathbb{Z} with Prime numbers at the base of each strand. This structure shows more clearly if we leave out the Composite strands of $2n$ and $3n$,

$n \in \mathbb{Z}$, and restrict ourselves to composite strands over the set $\{6n \pm 1\}$, where the strands are $z = x \cdot P_i$, for all Primes $P_i > 3$ and all integers x in $\{6n \pm 1\}$

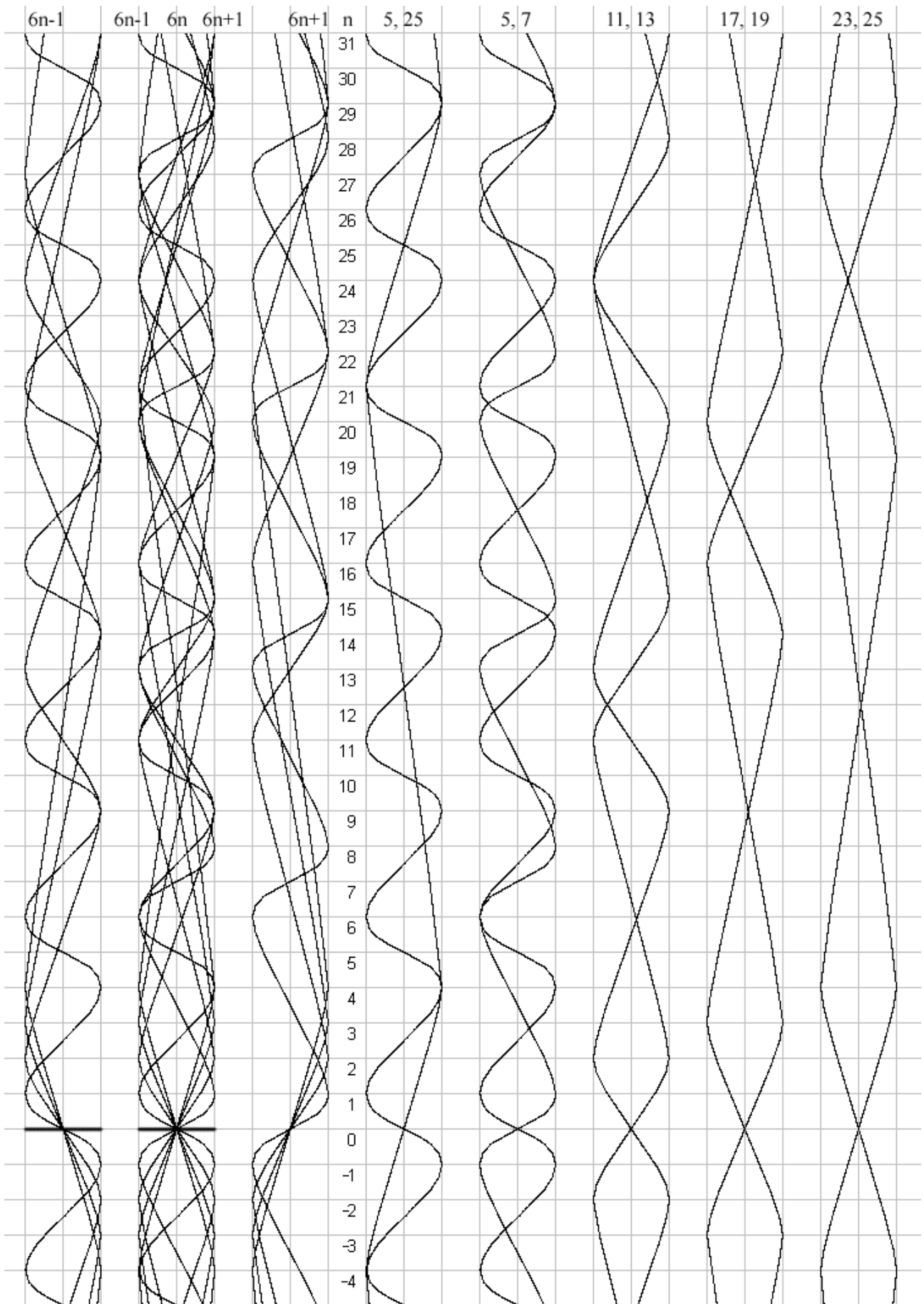


Fig 1-1: "Composite Strands of $\{6n \pm 1\}$ over $[-31, 187]$ "

Figure 1-1 shows stylised representations of the Composite strands over the set $\{6n \pm 1\}$ for the range $[-31, 187]$. Also, it does not include the Composite strands of 2 and 3. Each horizontal unit is of size 1. Each vertical unit is of size 6 and is referred to as a unit of size K , due to the PC Key function, $K(r)$, defined below. For clarity I have only included strands for $n=0, \pm 1, \pm 2, \pm 3, \pm 4$.

From left to right the graphs are Composite strands of:

- $\{6n - 1\}$,
- $\{6n \pm 1\}$,
- $\{6n + 1\}$,
- 5 and 25 {all intersections with $\{6n \pm 1\}$ of the strand of 25 overlap with the strand of 5}
- 5 and 7,
- 11 and 13
- 17 and 19
- 23 and 25

Just plotting these few strands shows part of why it has been so difficult to find the Structure of Primes over \mathbb{Z} ; Primes are indirectly related, and are the result of gaps in the Composite weave of smaller Primes

The Fundamental Theorem of Primes follows clearly from Theorem 4 and its Lattice structure of Composite Strands.

Theorem 7: Fundamental Theorem of Primes

All Integers are members of only one of the sets:

- Prime Base, $\mathbf{B} = \{\pm P_1, \pm P_2\} = \{-3, -2, 2, 3\}$
- Subtractive Primes, \mathbf{P}_s , of the form $2.3.n - 1, n \in \mathbb{Z}$
- Additive Primes, \mathbf{P}_A , of the form $2.3.n + 1, n \in \mathbb{Z}$
- Composites of the forms $2.n, 3.n, n \in \mathbb{Z}, |n| \neq 1$, ie Multiples of 2 and/or 3, includes 0
- Composites, of the form $2.3.n \pm 1, n \in \mathbb{Z}$, ie Multiples of Primes other than 2 or 3

I term the set, $\{6n \pm 1\}$, the Prime Candidates (PC), \mathbf{P} .

As Primes form the basis for this Lattice structure of Composite strands, I shall formally refer to it as the “Prime Lattice”.

n is the Prime Candidates (PC) Integer Key value.

r , from the Prime Real Form Theorem, is the PC Real Key value

The Prime numbers, \mathbf{P} are a subset of the union of \mathbf{B} and \mathbf{P} .

$$\mathbf{P} \subset \mathbf{B} \cup \mathbf{P} = \mathbf{B} \cup \mathbf{S} \cup \mathbf{A} \text{ such that}$$

$$\begin{aligned} \mathbf{B} &= \{ \pm 2, \pm 3 \} \\ \mathbf{S} &= 6n - 1, \quad n \in \mathbb{Z} \\ \mathbf{A} &= 6n + 1, \quad n \in \mathbb{Z} \end{aligned}$$

where \mathbf{B} is the Prime Base set, \mathbf{S} is the Subtractive Prime Candidates set and \mathbf{A} is the Additive Prime Candidates set

Integers that are not elements of \mathbf{P} are multiples of 2 and/or 3, ie other than ± 2 and ± 3 , such integers are not candidates for being Prime numbers. Any Integers in \mathbf{P} are candidates for testing when searching for Primes and as such are termed Prime Candidates.

The Theorem of Prime Candidate Holes is a corollary to the Fundamental Theorem of Primes, and follows clearly, by observation, from Table 1-1 and Figure 1-1

Theorem 8: Prime Candidate Holes

$x = 6n \pm 1$ is Prime iff it is not the intersection of a Composite strand of a smaller Prime Candidate, $x' = 6m \pm 1$, with the Prime Candidate Set, $\forall n, m \in \mathbb{Z}, 0 < |m| < |n|$

This is really just the Sieve of Eratosthenes restricted to the Prime Candidate set and can be equivalently stated as:

Theorem 9: Prime PCs

$x = 6n \pm 1$ is Prime iff it is not the product of a smaller Prime Candidate, $x' = 6m \pm 1$, $\forall n, m \in \mathbb{Z}, 0 < |m| < |n|$

Let P_i^\pm be the i^{th} Subtractive or Additive Prime Candidate, $P_i^\pm = 6i \pm 1$, $P_i^- = 6i - 1$, $P_i^+ = 6i + 1$, $i \in \mathbb{Z}$.

Define the PC Key function $K(r)$ st

- 1) $K(r) = \lfloor \frac{(r+1)}{6} \rfloor, r \in \mathbb{R}, r \geq 0$
- 2) $K(r) = \lfloor \frac{(r-1)}{6} \rfloor, r \in \mathbb{R}^-$

Therefore, $\forall i \in \mathbb{N}$,

$$K(P_i^-) = i$$

$$K(P_i^+) = i$$

$$K(P_i^\pm) = i$$

$K(r)$ is the “distance” of r from zero in terms of Prime Candidate Integer Key values

Define the Inverse PC Key function $P^\pm(r)$ st

- 1) $P^+(r) = 6[r] + 1, r \in \mathbb{R}, r \geq 0$
- 2) $P^-(r) = 6[r] - 1, r \in \mathbb{R}, r \geq 0$
- 1) $P^+(r) = 6[r] + 1, r \in \mathbb{R}^-$
- 2) $P^-(r) = 6[r] - 1, r \in \mathbb{R}^-$

Therefore, $\forall i \in \mathbb{N}$,

$$P^-(i) = P_i^-$$

$$P^+(i) = P_i^+$$

$$P^\pm(i) = P_i^\pm$$

For PC Key value of 0, $P_0^- = -1, P_0^+ = 1$

$$P_0^- \times P_0^- = P_0^+, \text{ ie } -1 \times -1 = 1 \in \mathbf{A}$$

$$P_0^+ \times P_0^- = P_0^-, \text{ ie } 1 \times -1 = -1 \in \mathbf{S}$$

As mentioned at the start of this paper, it is common practice, [Ingham, 1932] and [Jameson, 2003], that 1 is considered as neither Prime nor Composite. Now I extend that to include -1, as P_0^\pm will be

considered as neither Prime nor Composite.

Set Properties of the Prime Candidates, \mathcal{P}

Let $\mathbf{B} \times \mathcal{P}$ denote the Composite set generated by multiplying $b \times p, \forall b \in \mathbf{B}, \forall p \in \mathcal{P}$

$$\mathbb{Z} = \{2n, 3n\} \cup \mathcal{P}, n \in \mathbb{Z},$$

$$\{2n, 3n\} \cap \{\mathcal{S} \cup \mathcal{A}\} = \{\}, n \in \mathbb{Z}$$

$$\mathbf{B} \times \mathcal{P} \not\subset \mathcal{P}$$

$$\mathcal{S} \times \mathcal{S} \subset \mathcal{A}$$

$$\mathcal{A} \times \mathcal{A} \subset \mathcal{A}$$

$$\mathcal{S} \times \mathcal{A} \subset \mathcal{S}$$

$$\mathcal{S} = -1 \times \mathcal{A}$$

$$\mathcal{A} = -1 \times \mathcal{S}$$

$$\{\mathcal{S} \times \mathcal{S}\} \cap \{\mathcal{A} \times \mathcal{A}\} \neq \{\}$$

$$\{\mathcal{S} \times \mathcal{S}\} \cup \{\mathcal{A} \times \mathcal{A}\} \cup \mathcal{P}_{\mathcal{A}} = \mathcal{A}, \text{ by the Fundamental Theorems of Primes, and of Arithmetic}$$

$$\{\mathcal{S} \times \mathcal{A}\} \cup \mathcal{P}_{\mathcal{S}} = \mathcal{S}, \text{ by the Fundamental Theorems of Primes, and of Arithmetic}$$

Intersection of Composite Strands with $6n \pm 1$

Where will the Composite strand of Subtractive Prime Candidate $(6n-1)$ intersect with the Subtractive Prime Candidates $(6c-1)$? Let us restrict ourselves for the moment to (+)ve PCs, WLOG

The answer can be determined in a number of ways. Using the PC Lattice structure and then generalising,

$(6.0-1) = -1$	Starting Position for $n=0, (6 \times 0 - 1) = -1$
$(6.1-1) = 5$	Starting Position for $n=1, (6 \times 1 - 1) = 5$
$(6.2-1) = 11$	Starting Position for $n=2, (6 \times 2 - 1) = 11$
$(6.3-1) = 17$	
$(6.4-1) = 23$	
$(6.5-1) = 29$	
$(6.6-1) = 35$	First Intersection for strand of $n=1, (6 \times (1+5) - 1) = 6 \times 6 - 1 = 36 - 1$
$(6.7-1) = 41$	
$(6.8-1) = 47$	
$(6.9-1) = 53$	
$(6.10-1) = 59$	
$(6.11-1) = 65$	Second Intersection for strand $n=1, (6 \times (1+2 \times 5) - 1) = 6 \times 11 - 1 = 66 - 1$
$(6.12-1) = 71$	
$(6.13-1) = 77$	First Intersection for strand $n=2, (6 \times (2+11) - 1) = 6 \times 13 - 1 = 78 - 1$
$(6.14-1) = 83$	
$(6.15-1) = 89$	
$(6.16-1) = 95$	Third Intersection for strand $n=1, (6 \times (1+3 \times 5) - 1) = 6 \times 16 - 1 = 96 - 1$

Subtractive PC $6n-1$, with PC Key value n , intersects with the Subtractive PCs at
 $6n - 1$
 $6(n+(6n-1)) - 1$

$$6(n+2(6n-1)) - 1$$

...

$$\begin{aligned} 6c-1 &= 6(n+m(6n-1)) - 1 \\ &= 6n + 6m(6n-1) - 1 \\ &= 6m(6n-1) + (6n - 1) \\ &= (6m+1)(6n-1) \end{aligned}$$

Generalising; any Subtractive Prime Candidate Composite strand, $(6n-1)$, will intersect with the Subtractive Prime Candidates at Additive Prime Candidate multiples, $(6c-1) = (6n-1)(6m+1)$.

$$\begin{aligned} \text{For } P_n^- &= 6n - 1, \\ 6c-1 &= (6n - 1)(6m+1) \\ &= 6mP_n^- + 6n - 1 \\ &= 6(mP_n^- + n) - 1 \\ c &= mP_n^- + n && [= -(mP_n^+ + (-n))] \end{aligned}$$

It follows that any Additive Prime Candidate Composite strand, $(6m+1)$, will intersect with the Subtractive Prime Candidates at Subtractive Prime Candidate multiples, $(6c-1) = (6n-1)(6m+1)$.

$$\begin{aligned} \text{For } P_m^+ &= 6m + 1, \\ 6c-1 &= (6m + 1)(6n-1) \\ &= 6nP_m^+ - 6m - 1 \\ &= 6(nP_m^+ - m) - 1 \\ c &= nP_m^+ - m && [= -(nP_m^- - (-m))] \end{aligned}$$

Any Subtractive Prime Candidate Composite strand, $(6n-1)$, will intersect with the Additive Prime Candidates at Subtractive Prime Candidate multiples, $(6c+1) = (6n-1)(6m-1)$.

$$\begin{aligned} \text{For } P_n^- &= 6n - 1, \\ 6c+1 &= (6n - 1)(6m-1) \\ &= 6mP_n^- - 6n + 1 \\ &= 6(mP_n^- - n) + 1 \\ c &= mP_n^- - n && [= -(mP_n^+ - (-n))] \end{aligned}$$

Any Additive Prime Candidate Composite strand, $(6n-1)$, will intersect with the Additive Prime Candidates at Additive Prime Candidate multiples, $(6c+1) = (6n+1)(6m+1)$.

$$\begin{aligned} \text{For } P_m^+ &= 6m + 1, \\ 6c+1 &= (6m + 1)(6n+1) \\ &= 6nP_m^+ + 6m + 1 \\ &= 6(nP_m^+ + m) + 1 \\ c &= nP_m^+ + m && [= -(nP_m^- + (-m))] \end{aligned}$$

Section 2: Prime Density and the Prime Number Theorem

The Prime Number Theorem approximates the number of primes that are less than a given number n [Ingham 1932] [Jameson 2003] [Weisstein (2)]

Theorem 10: Prime Number Theorem

The number of primes that are less than a given number n is approximately $n/\ln(n)$,

$$\pi(n) \approx \frac{n}{\ln(n)}$$

It's clear now why the density of Prime Numbers decreases as n increases; the Prime Candidate Strands (multiples) of P_n^\pm intersect with the Prime Candidate Set and prevent a Prime Candidate from being Prime, resulting in fewer Prime Candidate Holes as z increases. Euclid's Proof though, shows that existing Composite strands do not fill all of the Prime Candidate Set but instead must always leave Prime Holes forming the start of new Composite strands over \mathbf{P}

While this cause is straightforward, its effect is not. Attempts to calculate the Number of Primes by Combinatorial methods based on this structure are quickly affected by Complexity Theory. This simple structure has quite tangled results

We shall restrict ourselves to the (+)ve Integers and disregard PC Integer Key value 0 as $P_0^+=1$ is considered to be neither Prime nor Composite and does not generate Composite Prime Candidates, cf *Section 1: The Structure of Primes over \mathbb{Z}*

For each (+)ve integer c there will be:

$4c-2$ Composite (+)ve multiples of 2 and/or 3 which are less than $P_c^+=6c+1$

c (+)ve Subtractive PCs less than or equal to P_c^-

c (+)ve Additive PCs less than or equal to P_c^+ , and greater than P_0^+

ie $\exists c P_i^-$ and $c P_i^+$ st $0 < i \leq c$

$K(6c\pm 1) = c$, where K is the PC Integer Key Function

The smallest Subtractive PC that generates Composite PCs is $P_1^-=5$

The smallest Additive PC that generates Composite PCs is $P_1^+=7$

If P_1^- generates a Composite PC, P_z^\pm , less than or equal to $6c-1$ then there must be a PC co-factor, P_{F1}^\pm , st

$$P_z^\pm = P_1^\pm \times P_{F1}^\pm$$

$$K(P_{F1}^\pm) = K\left(\frac{P_c^\pm}{5}\right)$$

There are two (+)ve PCs for each PC Integer Key value. 5×1 is Prime, so there are approximately $2 \times K(P_{F1}^\pm) - 1$ Composite PC products of 5 that are less than, or equal to, P_c^+

If P_1^+ generates a Composite PC, P_y^\pm , less than or equal to $6c-1$ then there must be a PC co-factor, P_{F1}^\pm , st

$$K(P_{F1+}^{\pm}) = K\left(\frac{P_c^{\pm}}{7}\right)$$

There are two (+)ve PCs for each PC Integer Key value. 7x1 is Prime, 7x5 is an overlap with the composites of 5, so there are approximately $2 \times K(P_{F1+}^{\pm}) - 2$ Composite PC products of 7 that are less than, or equal to, P_c^+ and have not already been counted

P_{F1-}^{\pm} is the largest PC which generates Composite PCs less than or equal to P_c^+ , but its PC co-factor, 5, has already been counted. Similarly, P_{F1+}^{\pm} has the co-factor 7 which has already been counted

We would then proceed to repeat the above arguments for each Composite strand in turn

If P_2^- generates a Composite PC, P_x^{\pm} , less than or equal to $6c-1$ then there must be a PC co-factor, P_{F2-}^{\pm} , st

$$K(P_{F2-}^{\pm}) = K\left(\frac{P_c^{\pm}}{11}\right)$$

11x1 is Prime, 11x5 and 11x7 are overlaps with the composites of 5 and 7, so there are approximately $2 \times K(P_{F1-}^{\pm}) - 3$ Composite PC products of 7 that are less than, or equal to, P_c^+ and have not already been counted

This then becomes the basis for the algorithm of a sieve for working out the number of Composites less than P_c^+ and then subtracting that quantity from the $2c$ Prime Candidates in question. This algorithm demonstrates the validity of the Prime Structure and opens up further areas of investigation. As an approximation to the Number of Composites less than P_c^+ , though, it is a resource intensive approach that proves infeasible for large numbers.

From Figure 1-1 we can see that every PC product of 25 is also a product of 5. Similarly, 35 intersects with the Prime Candidates every time the strands of 5 and 7 intersect with the same PC. 49 doubles up with 7, 1001 overlaps with the strands of 7, 11 and 13; etc. Thus the algorithm would need to identify, and discard, Composite PC strands as any Composite PCs generated by them have already been counted against the strands of their prime sub-factors. This requires resources to remember Primes found so far and to work out whether a strand is composite as one of the first steps in each iteration of this algorithm

An alternative approach, Plateaus at Powers of P

Another way to approach this problem is based on the Unique Factorisation Theorem with plateaus at powers of the first Prime Candidate, 5. Considering (+)ve Powers of 5:

5^1	=	5	2 Primes < 5
5^2	=	25	7 Primes between 5 & 25 inclusive
5^3	=	125	21 Primes between 25 & 125 inclusive, $21=7 \times 3$
5^4	=	625	84 Primes between 125 & 625 inclusive, $84=7 \times 3 \times 4$
5^5	=	3,125	
5^6	=	15,625	
5^7	=	78,125	
5^8	=	390,625	
5^9	=	1,953,125	
5^{10}	=	9,765,625	

$$\underline{5^1 = 5}$$

1xP=P, therefore 1 does not generate Composite PCs

There are 2 Primes less than 5: 2 and 3

$$\underline{5^2 = 25}$$

5 is the smallest Prime PC that generates Composite PCs and 5x5 is the smallest Composite Prime PC

There are no multiples of PCs which have Product less than 25

25 is additive & $K(25) = 4$, therefore there are $2 \times 4 - 1 = 7$ Prime PCs less than 25

Thus, there are 7 Prime PCs less than 25, for a total of 9 Primes less than 25

$$\underline{5^3 = 125}$$

$5 \times 5 \times 5 = 125$ is smallest Composite Prime PC with 3 PC factors

125 is Subtractive & $K(125) = 21$, therefore there are, at most, $2 \times (21 - 1 - 4) = 32$ Prime PCs strictly between 25 & 125, non-inclusive

Taking the 6 PCs between 5 and 25, $5 < P < 25 \Rightarrow 25 < 5 \times P < 125$, therefore 6 more Composites, ie there are at most 26 Prime PCs in this range

$$7 \times 5 = 35 < 125$$

$$7 \times 17 = 119 < 125$$

$$7 \times 19 = 133 > 125$$

17 is subtractive & $K(17) = 3$, thus $2 \times 3 - 1 - 1 = 4$ more Composites (5P has already been counted) ie between 7 & 28 Primes < 125

$$11 \times 11 = 121 < 125$$

Thus 1 more Composite

Therefore

$$\underline{5^4 = 625}$$

$$\underline{5^5 = 3125}$$

	<i>Base</i>	<i>Power</i>
	5^1	5
	5^1	25
	5^1	125
	5^1	625
	5^1	3125
	5^1	
	5^1	
	5^1	

Section 3: Factoring Composites

In this Section Prime Factorisation equations are derived from the structure of Primes.

$$\mathbb{Z} = \{2n, 3n\} \cup S \cup A, \quad n \in \mathbb{Z}$$

Composite strands of ± 2 and ± 3 do not intersect with the Prime Candidates

Derivation of the Factorisation equations

Subtractive Prime Candidates are of the form $6c-1$. **IF** $6c-1$ is not Prime then $6c-1 = (6n-1)(6m+1)$ has non-trivial Integer solutions for all 3 PC Key values c, n, m .

Solving for PC Key value m

From the “*Intersection of Composite Strands with $6n \pm 1$* ”, above

$$\begin{aligned}c &= mP_n^- + n \\m(6n-1) &= c-n\end{aligned}$$

$$m = \frac{c-n}{6n-1}$$

IF $(6c-1)$ is a multiple of $(6n-1)$ then $(c-n)$ is a multiple of $(6n-1)$ and

$$\begin{aligned}(c-n) \bmod (6n-1) &\equiv 0 \\c \bmod (6n-1) &\equiv n\end{aligned}$$

$$\begin{aligned}6c-1 \bmod (6n-1) &\equiv 0 \\6c \bmod (6n-1) &\equiv 1\end{aligned}$$

Also, IF $(c-n)$ is NOT a multiple of $(6n-1)$ then $(6c-1)$ is NOT a multiple of $(6n-1)$ and

$$\begin{aligned}(c-n) \bmod (6n-1) &\neq 0 \\c \bmod (6n-1) &\neq n \\6c-1 \bmod (6n-1) &\neq 0 \\6c \bmod (6n-1) &\neq 1\end{aligned}$$

Solving for PC Key value n

From the “*Intersection of Composite Strands with $6n \pm 1$* ”, above

$$\begin{aligned}c &= nP_m^+ - m \\n(6m+1) &= c+m\end{aligned}$$

$$n = \frac{c+m}{6m+1}$$

IF $(6c-1)$ is a multiple of $(6m+1)$ then $(c+m)$ is a multiple of $(6m+1)$ and

$$\begin{aligned}(c+m) \bmod (6m+1) &\equiv 0 \\c \bmod (6m+1) &\equiv -m\end{aligned}$$

$$\begin{aligned}6c-1 \bmod (6m+1) &\equiv 0 \\6c \bmod (6m+1) &\equiv 1\end{aligned}$$

Also, IF $(c+m)$ is NOT a multiple of $(6m+1)$ then $(6c-1)$ is NOT a multiple of $(6m+1)$ and

$$\begin{aligned}(c+m) \bmod (6m+1) &\neq 0 \\c \bmod (6m+1) &\neq -m\end{aligned}$$

$$6c-1 \pmod{(6m+1)} \neq 0$$

$$6c \pmod{(6m+1)} \neq 1$$

Additive Prime Candidates are of the form $6c+1$. **IF** $6c+1$ is not Prime then either

$$1) 6c+1 = (6n-1)(6m-1), \quad \text{or,}$$

$$2) 6c+1 = (6n+1)(6m+1)$$

have non-trivial Integer solutions for all 3 PC Key values c, n, m .

In each case we need only solve for one term, n or m , WLOG

Case 1) Product of Subtractive Prime Candidates: Solving for PC Key value m

From the "*Intersection of Composite Strands with $6n\pm 1$* ", above

$$c = mP_n^- - n$$

$$m(6n-1) = c+n$$

$$m = \frac{c+n}{6n-1}$$

IF $(6c+1)$ is a multiple of $(6n-1)$ then $(c+n)$ is a multiple of $(6n-1)$ and

$$(c+n) \pmod{(6n-1)} \equiv 0$$

$$c \pmod{(6n-1)} \equiv -n$$

$$6c-1 \pmod{(6n-1)} \equiv 0$$

$$6c \pmod{(6n-1)} \equiv 1$$

Also, IF $(c+n)$ is NOT a multiple of $(6n-1)$ then $(6c+1)$ is NOT a multiple of $(6n-1)$ and

$$(c+n) \pmod{(6n-1)} \neq 0$$

$$c \pmod{(6n-1)} \neq -n$$

$$6c-1 \pmod{(6n-1)} \neq 0$$

$$6c \pmod{(6n-1)} \neq 1$$

Case 2) Product of Additive Prime Candidates: Solving for PC Key value n

From the "*Intersection of Composite Strands with $6n\pm 1$* ", above

$$c = nP_m^+ + m$$

$$n(6m+1) = c-m$$

$$n = \frac{c-m}{6m+1}$$

IF $(6c+1)$ is a multiple of $(6m+1)$ then $(c-m)$ is a multiple of $(6m+1)$ and

$$(c-m) \pmod{(6m+1)} \equiv 0$$

$$c \pmod{(6m+1)} \equiv m$$

$$6c+1 \pmod{(6m+1)} \equiv 0$$

$$6c \pmod{(6m+1)} \equiv -1$$

Also, IF $(c-m)$ is NOT a multiple of $(6m+1)$ then $(6c+1)$ is NOT a multiple of $(6m+1)$ and

$$(c-m) \pmod{(6m+1)} \neq 0$$

$$\begin{aligned}c \bmod (6m+1) &\neq m \\6c+1 \bmod (6m+1) &\neq 0 \\6c \bmod (6m+1) &\neq -1\end{aligned}$$

Note: P_n^\pm and P_m^\pm may be themselves be Composite Prime Candidates for some, but not all, values of n and m . There must be at least one n and m for which these PCs are not Composite, even if it is for PC Key values of 1 and C

The symmetry in the equations for n and m is because

$$\begin{aligned}\mathbf{S} &= -1 \times \mathbf{A}, & 6n-1 &= -1 \times (6(-n) + 1) \\ \mathbf{A} &= -1 \times \mathbf{S}, & 6m+1 &= -1 \times (6(-m) - 1)\end{aligned}$$

Selecting Initial PC Key values

For any positive Integer, $z=x \cdot y$, WLOG, $x \leq \sqrt{z}$ and $y \geq \sqrt{z}$

For any positive Composite Subtractive Prime Candidate, $z = 6c-1$

$$z = (6n-1)(6m+1), \quad (6n-1) \neq (6m+1),$$

so either,

$$\begin{aligned}(6n-1) &< \sqrt{6c-1} \quad \text{and} \quad (6m+1) > \sqrt{6c-1}, \\ n &\leq \lfloor \frac{(1+\sqrt{6c-1})}{6} \rfloor < \frac{1}{6} + \frac{\sqrt{6c}}{6} < 1 + \lfloor \frac{\sqrt{c}}{\sqrt{6}} \rfloor\end{aligned}$$

Set n to one of the 3 values above

or

$$\begin{aligned}(6m+1) &< \sqrt{6c-1} \quad \text{and} \quad (6n-1) > \sqrt{6c-1}, \\ m &\leq \lfloor \frac{(\sqrt{6c-1})-1}{6} \rfloor < \frac{\sqrt{6c}}{6} \leq \lfloor \frac{\sqrt{c}}{\sqrt{6}} \rfloor\end{aligned}$$

Set m to one of the 3 values above

As we don't know which value is less, n or m , we need to test against both. It would be safe to initialise m to n , as the initial bound for n is approximately one greater than for m

For any positive Composite Additive Prime Candidate, $z = 6c+1$,

$$z = (6n-1)(6m-1), \quad (6n-1) \leq \sqrt{z} \quad \text{WLOG},$$

or

$$z = (6n+1)(6m+1), \quad (6m+1) \leq \sqrt{z} \quad \text{WLOG},$$

so either,

$$\begin{aligned}(6m-1) &\leq \sqrt{6c+1}, \quad \text{WLOG} \\ m &\leq \lfloor \frac{1+(\sqrt{6c+1})}{6} \rfloor < \frac{1}{6} + \frac{(\sqrt{6c})+1}{6} \leq 1 + \lfloor \frac{\sqrt{c}}{\sqrt{6}} \rfloor\end{aligned}$$

Set m to one of the 3 values above

or

$$\begin{aligned}(6n+1) &\leq \sqrt{6c+1}, \quad \text{WLOG} \\ n &\leq \lfloor \frac{(\sqrt{6c+1})-1}{6} \rfloor \leq \frac{\sqrt{6c}}{6} \leq \lfloor \frac{\sqrt{c}}{\sqrt{6}} \rfloor\end{aligned}$$

Set n to one of the 3 values above

As we don't know whether z is the product of Additive or Subtractive Prime Candidates, we need to test against both n and m . It would be safe to initialise n to m , as the initial bound for m is approximately one greater than for n

$$\text{Initial PC Key value} = \psi = 1 + \left\lceil \frac{\sqrt{c}}{\sqrt{6}} \right\rceil$$

In both cases, factoring a Subtractive or an Additive PC, one can safely use this value as the Initial PC Key value

Structured Factorisation Algorithm

To factorise $z \in \mathbb{Z}$ into factors $z = (-1)^{E_1} \cdot 2^{E_2} \cdot 3^{E_3} \cdot 5^{E_4} \cdot \dots \cdot P_i^{E_i}$

- 1) If z is negative then $E_1=1$. Set z to positive, $z=|z|$ Otherwise $E_1=0$.
- 2) While z is odd divide z by 2 until the result is odd to obtain E_2 , the Power to which 2 is a factor of z
- 3) Divide z by 3 until z is indivisible by 3 to obtain E_3
- 4) At this stage z is without factors of 2 or 3 and thus is a Prime Candidate.

If $z=1$ then

Finished, $z = (-1)^{E_1} \cdot 2^{E_2} \cdot 3^{E_3}$

Else

Solve z modulo 6 to see whether z is a Subtractive ($z=6c-1$), or an Additive ($z=6c+1$) Prime Candidate

Note: In practice it may be faster to solve for $z+1$ or $z-1$

- 5) Solve for PC Key value c ,

Subtractive PC	$c=(z+1)/6$
Additive PC	$c=(z-1)/6$

Note: In practice Steps 4 and 5 would be merged

Select the required pair of Factorisation equations from one of the three variations below.

Implementation

	$z = 6c - 1$	$z = 6c + 1$
Division	$m = \frac{c - n}{6n - 1}$	$m = \frac{c + n}{6n - 1}$
	$n = \frac{c + m}{6m + 1}$	$n = \frac{c - m}{6m + 1}$
1 st Modulo (%)	$(c - n) \% (6n - 1) = 0$	$(c + n) \% (6n - 1) = 0$
	$(c + m) \% (6m + 1) = 0$	$(c - m) \% (6m + 1) = 0$

Implementation2nd Modulo (%)

$$z = 6c - 1$$

$$c \% (6n-1) = n$$

$$c \% (6m+1) = -m$$

$$z = 6c + 1$$

$$c \% (6n-1) = -n$$

$$c \% (6m+1) = m$$

Note:

$$c \% (6m+1) = -m = (c-m) \% (6m+1)$$

$$c \% (6n-1) = -n = (c-n) \% (6n-1)$$

6) Set n and m to the initial Prime Candidate Key Values,

$$\text{Initial PC Key value} = \psi = 1 + \left\lceil \frac{\sqrt{c}}{\sqrt{6}} \right\rceil$$

7) Solve the selected implementation for m and n

8) Decrement m and n

9) Repeat from Step 7 until either:

solved for an integral n or m, *the first solution, (which may be composites)*

or

n = m = 0, *all solutions*

The above algorithms require iteration through possible solutions in the hope that integer solutions are found. When factoring a Prime number, P, only the trivial solutions will be found, n=0 or m=0 giving $\pm 1, \pm P$. With large numbers, such as RSA-640 [RSA], we would need a massive number of iterations. Fortunately, these algorithms do allow massively parallel implementations, unfortunately, they are still a comparatively slow process.

For the equations $K = \frac{(c \pm n)}{(6n \pm 1)}$,

Over X computers, the ith computer, $0 < i < X$, would evaluate the range

$$n \in \left[(i-1) \cdot \left\lceil \frac{\psi}{X} \right\rceil + 1, i \cdot \left\lceil \frac{\psi}{X} \right\rceil \right]$$

The Xth computer need only evaluate

$$n \in \left[(X-1) \cdot \left\lceil \frac{\psi}{X} \right\rceil + 1, \psi \right]$$

Name: RSA-640

Digits: 193

Digit Sum: 806

31074182404900437213507500358885679300373460228427275457201619488232064405180815
 04556346829671723286782437916272838033415471073108501919548529007337724822783525
 742386454014691736602477652346609

Refer Appendix B for an implementation for factoring (6c-1)

Further Investigation into Factorisation Algorithms

A major issue with the above Factorisation Algorithm is that it is iterative and not direct. I have not been able to find a direct method of Factorisation, but have investigated other iterative algorithms.

Lemma 1: Prime Candidate Expansion

All Prime Candidates, $6n - 1$ or $6m + 1$, may be expressed in the form $6a \pm 6b - 1$ or $6c \pm 6d + 1$, respectively, where $a \pm b = n$, $c \pm d = m$ $a, b \in \mathbb{Z}$

Factoring Subtractive Prime Candidates

As stated previously, Subtractive PCs are of the form $6x - 1$. **IF** $6x - 1$ is not Prime then $6x - 1 = (6n - 1)(6m + 1)$ has non-trivial Integer solutions for all 3 PC Key values x, n, m .

Let $z = 6x - 1 = (6n - 1) \cdot (6m + 1)$

$$\begin{aligned} z &= (5 + 6b_1) \cdot (7 + 6d_1), \text{ by Lemma 1. ie, if } 6n - 1 = 5 - 6b \text{ then let } b_1 = -b. \text{ Solve for } b_1 \text{ or } d_1 \\ &= (11 + 6b_2) \cdot (7 + 6d_1), \text{ solve for } b_2 \text{ or } d_1 \\ &= (11 + 6b_2) \cdot (13 + 6d_2), \text{ solve for } b_2 \text{ or } d_2 \\ &= (\{6a - 1\} + 6b_A) \cdot (\{6c + 1\} + 6d_C), \text{ solve for } b_A \text{ or } d_C \end{aligned}$$

Select values for a and b:

$\{6a - 1\}$ and $\{6c + 1\}$ will be fixed, or constant, for selected, fixed, a and b

Let $E = \{6a - 1\}$, $F = \{6c + 1\}$, E and F are Prime Candidates

$$E \cdot F = 6a \cdot 6c + 6a - 6c - 1$$

$$\begin{aligned} 6x - 1 &= (E + 6b_A) \cdot (F + 6d_C) \\ 6x - 1 &= E \cdot F + E \cdot 6d_C + F \cdot 6b_A + 6b_A \cdot 6d_C \\ 6x - 1 - E \cdot F &= E \cdot 6d_C + F \cdot 6b_A + 6b_A \cdot 6d_C \end{aligned}$$

$$\begin{aligned} 6x - 1 - 6a \cdot 6c - 6a + 6c + 1 &= E \cdot 6d_C + F \cdot 6b_A + 6b_A \cdot 6d_C \\ 6x - 6a \cdot 6c - 6a + 6c &= E \cdot 6d_C + F \cdot 6b_A + 6b_A \cdot 6d_C \\ 6(x - 6a \cdot c - a + c) &= E \cdot 6d_C + F \cdot 6b_A + 6b_A \cdot 6d_C \end{aligned}$$

Let $k = (x - 6a \cdot c - a + c)$, k is a constant for fixed a, c

$$6k = E \cdot 6d_C + F \cdot 6b_A + 6b_A \cdot 6d_C$$

$$k = E \cdot d_C + F \cdot b_A + 6b_A \cdot d_C$$

$$1) \quad k = d_C (E + 6b_A) + F \cdot b_A$$

$$d_C = \frac{(k - F \cdot b_A)}{(E + 6b_A)}$$

$$2) \quad k = E \cdot d_C + b_A (F + 6d_C)$$

$$b_A = \frac{(k - E \cdot d_C)}{(F + 6d_C)}$$

With this Generalised Factorisation Algorithm:

- 1) there can be an infinite number of simultaneous equations for the factorisation of a number, subject to the values selected for a and c.
- 2) a and c may be any selected, fixed, Integer values, solve with iterations performed over b_A and d_C
- 3) b_A and d_C may be fixed, solve with iterations performed over a and c

Similar algorithms exist for factoring Additive PCs

Factoring Additive Prime Candidates

As stated previously, Additive PCs are of the form $6x+1$. **IF** $6x+1$ is not Prime then either

- 1) $6x+1 = (6n-1)(6m-1)$, or,
- 2) $6x+1 = (6n+1)(6m+1)$

have non-trivial Integer solutions for all 3 PC Key values x, n, m .

In each case we need only solve for one term, n or m , WLOG

Case 1) Product of Subtractive Prime Candidates:

Let $z = 6x+1 = (6n-1) \cdot (6m-1)$

$z = (5 + 6b_1) \cdot (5 + 6d_1)$, by Lemma 1. ie, if $6n-1 = 5-6b$ then let $b_1 = -b$. Solve for b_1 or d_1

$= (11 + 6b_2) \cdot (5 + 6d_1)$, solve for b_2 or d_1

$= (11 + 6b_2) \cdot (11 + 6d_2)$, solve for b_2 or d_2

$= (\{6a - 1\} + 6b_A) \cdot (\{6c - 1\} + 6d_C)$, solve for b_A or d_C

Select values for a and b :

$\{6a - 1\}$ and $\{6c - 1\}$ will be fixed, or constant, for selected, fixed, a and b

Let $E = \{6a - 1\}$, $F = \{6c - 1\}$, E and F are Prime Candidates

$E \cdot F = 6a \cdot 6c - 6a - 6c + 1$

$$6x + 1 = (E + 6b_A) \cdot (F + 6d_C)$$

$$6x + 1 = E \cdot F + E \cdot 6d_C + F \cdot 6b_A + 6b_A \cdot 6d_C$$

$$6x + 1 - E \cdot F = E \cdot 6d_C + F \cdot 6b_A + 6b_A \cdot 6d_C$$

$$6x + 1 - 6a \cdot 6c + 6a + 6c - 1 = E \cdot 6d_C + F \cdot 6b_A + 6b_A \cdot 6d_C$$

$$6x - 6a \cdot 6c + 6a + 6c = E \cdot 6d_C + F \cdot 6b_A + 6b_A \cdot 6d_C$$

$$6(x - 6a \cdot c + a + c) = E \cdot 6d_C + F \cdot 6b_A + 6b_A \cdot 6d_C$$

Let $k = (x - 6a \cdot c + a + c)$, k is a constant for fixed a, c

$$6k = E \cdot 6d_C + F \cdot 6b_A + 6b_A \cdot 6d_C$$

$$k = E \cdot d_C + F \cdot b_A + 6b_A \cdot d_C$$

$$1) \quad k = d_C (E + 6b_A) + F \cdot b_A$$

$$d_C = \frac{(k - F \cdot b_A)}{(E + 6b_A)}$$

$$2) \quad k = E \cdot d_C + b_A (F + 6d_C)$$

$$b_A = \frac{(k - E \cdot d_C)}{(F + 6d_C)}$$

Case 2) Product of Additive Prime Candidates:

Let $z = 6x+1 = (6n+1) \cdot (6m+1)$

$z = (7 + 6b_1) \cdot (7 + 6d_1)$, by Lemma 1. ie, if $6n+1 = 7-6b$ then let $b_1 = -b$. Solve for b_1 or d_1

$= (13 + 6b_2) \cdot (7 + 6d_1)$, solve for b_2 or d_1

$= (13 + 6b_2) \cdot (13 + 6d_2)$, solve for b_2 or d_2

$= (\{6a + 1\} + 6b_A) \cdot (\{6c + 1\} + 6d_C)$, solve for b_A or d_C

Select values for a and b :

$\{6a + 1\}$ and $\{6c + 1\}$ will be fixed, or constant, for selected, fixed, a and b

Let $E = \{6a + 1\}$, $F = \{6c + 1\}$, E and F are Prime Candidates

$E \cdot F = 6a \cdot 6c + 6a + 6c + 1$

$$6x + 1 = (E + 6b_A) \cdot (F + 6d_C)$$

$$6x + 1 = E.F + E.6d_C + F.6b_A + 6b_A.6d_C$$

$$6x + 1 - E.F = E.6d_C + F.6b_A + 6b_A.6d_C$$

$$6x + 1 - 6a.6c - 6a - 6c - 1 = E.6d_C + F.6b_A + 6b_A.6d_C$$

$$6x - 6a.6c - 6a - 6c = E.6d_C + F.6b_A + 6b_A.6d_C$$

$$6(x - 6a.c - a - c) = E.6d_C + F.6b_A + 6b_A.6d_C$$

Let $k = (x - 6a.c - a - c)$, k is a constant for fixed a, c

$$6k = E.6d_C + F.6b_A + 6b_A.6d_C$$

$$k = E.d_C + F.b_A + 6b_A.d_C$$

$$1) \quad k = d_C (E + 6b_A) + F.b_A$$

$$d_C = \frac{(k - F.b_A)}{(E + 6b_A)}$$

$$2) \quad k = E.d_C + b_A (F + 6d_C)$$

$$b_A = \frac{(k - E.d_C)}{(F + 6d_C)}$$

By using the same additive structure for the equation of $z = (\{6a \pm 1\} + 6b_A) \cdot (\{6c \pm 1\} + 6d_C)$ we end up with the same two equations across all three cases; factoring a Subtractive PC and both cases of factoring an Additive PC.

Alternatively, we could start from

$$z = (\{6a \pm 1\} - 6b_A) \cdot (\{6c \pm 1\} + 6d_C), \text{ or}$$

$$z = (\{6a \pm 1\} - 6b_A) \cdot (\{6c \pm 1\} - 6d_C)$$

and generate similar equations shared across the three cases. Whichever forms of the algorithms one used would depend on implementation or research dependencies

Trigonometric Representation of Factoring Algorithms

Though I have not been able to derive any improvements in Factoring, it is interesting to examine an

equation such as $m = \frac{c-n}{6n-1}$ in terms of Trigonometry. Given $(c-n) = (6n-1)m$, we are looking for the intersection of the constant line $y = (c-n)$ with the line $y = (6n-1)m$ and with c, n, m being integers

$y = c-n$ intersect $y = (6n-1)m$	$y = c-n$ intersect $y = m(6n-1)$
$x = m$	$x = 6n-1$
Slope = $6n-1$	Slope = m
Hypoteneuse ² = $(c-n)^2 + m^2$ = $c^2 - 2cn + n^2 + m^2$	Hypoteneuse ² = $(c-n)^2 + (6n-1)^2$ = $c^2 - 2n + n^2 + 36n^2 - 12n + 1$ = $37n^2 - 14n + c^2 + 1$
Hypoteneuse ² = $m^2(6n-1)^2 + m^2$ = $m^2 ((6n-1)^2 + 1)$ = $6^2.n^2m^2 - 12nm^2 + 2m^2$	Hypoteneuse ² = $m^2(6n-1)^2 + (6n-1)^2$ = $(6n-1)^2 (m^2 + 1)$ = $6^2.n^2m^2 - 12nm^2 + m^2 + 6^2.n^2 - 12n + 1$
Hypoteneuse ² = $(c-n)^2 / \text{Sin}(\theta_n)^2$ = $m^2 / \text{Cos}(\theta_n)^2$	Hypoteneuse ² = $(c-n)^2 / \text{Sin}(\theta_m)^2$ = $(6n-1)^2 / \text{Cos}(\theta_m)^2$

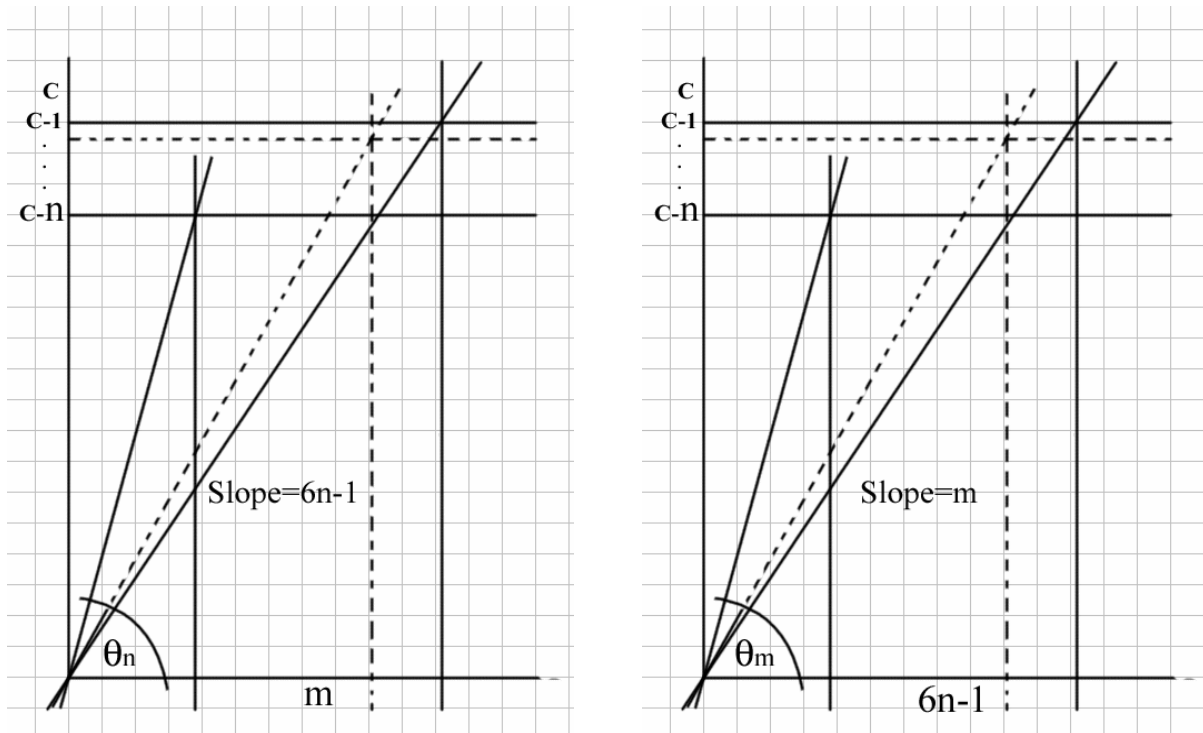


Fig 3-1: "Trigonometric Representations of $(c-n) = (6n-1)m$ "

Typically we are only interested in seeking Integer solutions for c , n and m . I am curious to see what use, if any, could be made of Real solutions.

All of the other Factorisation algorithms we have studied above may also be interpreted in terms of Trigonometric representations.

Section 4: PC Multiplication Charts

PC Multiplication charts demonstrate the relationships between PCs, especially when we look at the charts in terms of their PC Integer Key values

The difference between $(6n-1)x(6m+1)$ and $(6\{n+1\}-1)x(6m+1)$ is $6 + 36m = 6(6m+1)$

The difference between $(6n-1)x(6m+1)$ and $(6n-1)x(6\{m+1\}+1)$ is $-6 + 36n = 6(6n-1)$

	-11	-5	1	7	13	19
-25	275 -150 -66	125 -150 -30	-25 -150 6	-175 -150 42	-325 -150 78	-475 -150 114
-19	209 -114 -66	95 -114 -30	-19 -114 6	-133 -114 42	-247 -114 78	-361 -114 114
-13	143 -78 -66	65 -78 -30	-13 -78 6	-91 -78 42	-169 -78 78	-247 -78 114
-7	77 -42 -66	35 -42 -30	-7 -42 6	-49 -42 42	-91 -42 78	-133 -42 114
-1	11 -6 -66	5 -6 -30	-1 -6 6	-7 -6 42	-13 -6 78	-19 -6 114
5	-55 30 -66	-25 30 -30	5 30 6	35 30 42	65 30 78	95 30 114
11	-121 66 -66	-55 66 -30	11 66 6	77 66 42	143 66 78	209 66 114
17	-187 102 -66	-85 102 -30	17 102 6	119 102 42	221 102 78	323 102 114
23	-253 138 -66	-115 138 -30	23 138 6	161 138 42	299 138 78	437 138 114

Table 4-1: "Subtractive Row x Additive Column PC Multiplication Chart"

The difference between $(6n-1)x(6m-1)$ and $(6\{n+1\}-1)x(6m-1)$ is $-6 + 36m = 6(6m-1)$

The difference between $(6n-1)x(6m-1)$ and $(6n-1)x(6\{m+1\}-1)$ is $-6 + 36n = 6(6n-1)$

	-13	-7	-1	5	11	17
-25	325 -150 -78	175 -150 -42	25 -150 -6	-125 -150 30	-275 -150 66	-425 -150 102
-19	247 -114 -78	133 -114 -42	19 -114 -6	-95 -114 30	-209 -114 66	-323 -114 102
-13	169 -78 -78	91 -78 -42	13 -78 -6	-65 -78 30	-143 -78 66	-221 -78 102
-7	91 -42 -78	49 -42 -42	7 -42 -6	-35 -42 30	-77 -42 66	-119 -42 102
-1	13 -6 -78	7 -6 -42	1 -6 -6	-5 -6 30	-11 -6 66	-17 -6 102
5	-65 30 -78	-35 30 -42	-5 30 -6	25 30 30	55 30 66	85 30 102
11	-143 66 -78	-77 66 -42	-11 66 -6	55 66 30	121 66 66	187 66 102
17	-221 102 -78	-119 102 -42	-17 102 -6	85 102 30	187 102 66	289 102 102
23	-299 138 -78	-161 138 -42	-23 138 -6	115 138 30	253 138 66	391 138 102

Table 4-2: "Subtractive x Subtractive PC Multiplication Chart"

The difference between $(6n+1)x(6m+1)$ and $(6\{n+1\}+1)x(6m+1)$ is $6 + 36m = 6(6m+1)$

The difference between $(6n+1)x(6m+1)$ and $(6n+1)x(6\{m+1\}+1)$ is $6 + 36n = 6(6n+1)$

	-11	-5	1	7	13	19
-17	187 -102 -66	85 -102 -30	-17 -102 6	-119 -102 42	-221 -102 78	-323 -102 114
-11	121 -66 -66	55 -66 -30	-11 -66 6	-77 -66 42	-143 -66 78	-209 -66 114
-5	55 -30 -66	25 -30 -30	-5 -30 6	-35 -30 42	-65 -30 78	-95 -30 114
1	-11 6 -66	-5 6 -30	1 6 6	7 6 42	13 6 78	19 6 114
7	-77 42 -66	-35 42 -30	7 42 6	49 42 42	91 42 78	133 42 114
13	-143 78 -66	-65 78 -30	13 78 6	91 78 42	169 78 78	247 78 114
19	-209 114 -66	-95 114 -30	19 114 6	133 114 42	247 114 78	361 114 114
25	-275 150 -66	-125 150 -30	25 150 6	175 150 42	325 150 78	475 150 114
31	-341 186 -66	-155 186 -30	31 186 6	217 186 42	403 186 78	589 186 114

Table 4-3: "Additive x Additive PC Multiplication Chart"

	-2	-1	0	1	2	3						
-4	46	-25 -11	21	-25 -5	-4	-25 1	-29	-25 7	-54	-25 13	-79	-25 19
-3	35	-19 -11	16	-19 -5	-3	-19 1	-22	-19 7	-41	-19 13	-60	-19 19
-2	24	-13 -11	11	-13 -5	-2	-13 1	-15	-13 7	-28	-13 13	-41	-13 19
-1	13	-7 -11	6	-7 -5	-1	-7 1	-8	-7 7	-15	-7 13	-22	-7 19
0	2	-1 -11	1	-1 -5	0	-1 1	-1	-1 7	-2	-1 13	-3	-1 19
1	-9	5 -11	-4	5 -5	1	5 1	6	5 7	11	5 13	16	5 19
2	-20	11 -11	-9	11 -5	2	11 1	13	11 7	24	11 13	35	11 19
3	-31	17 -11	-14	17 -5	3	17 1	20	17 7	37	17 13	54	17 19
4	-42	23 -11	-19	23 -5	4	23 1	27	23 7	50	23 13	73	23 19

Table 4-4: "Subtractive Row x Additive Column Multiplication Chart in PC Key Values"

	-2	-1	0	1	2	3						
-4	54	-25 -13	29	-25 -7	4	-25 -1	-21	-25 5	-46	-25 11	-71	-25 17
-3	41	-19 -13	22	-19 -7	3	-19 -1	-16	-19 5	-35	-19 11	-54	-19 17
-2	28	-13 -13	15	-13 -7	2	-13 -1	-11	-13 5	-24	-13 11	-37	-13 17
-1	15	-7 -13	8	-7 -7	1	-7 -1	-6	-7 5	-13	-7 11	-20	-7 17
0	2	-1 -13	1	-1 -7	0	-1 -1	-1	-1 5	-2	-1 11	-3	-1 17
1	-11	5 -13	-6	5 -7	-1	5 -1	4	5 5	9	5 11	14	5 17
2	-24	11 -13	-13	11 -7	-2	11 -1	9	11 5	20	11 11	31	11 17
3	-37	17 -13	-20	17 -7	-3	17 -1	14	17 5	31	17 11	48	17 17
4	-50	23 -13	-27	23 -7	-4	23 -1	19	23 5	42	23 11	65	23 17

Table 4-5: "Subtractive x Subtractive PC Multiplication Chart in PC Key Values"

	-2	-1	0	1	2	3						
-4	42	-23 -11	19	-23 -5	-4	-23 1	-27	-23 7	-50	-23 13	-73	-23 19
-3	31	-17 -11	14	-17 -5	-3	-17 1	-20	-17 7	-37	-17 13	-54	-17 19
-2	20	-11 -11	9	-11 -5	-2	-11 1	-13	-11 7	-24	-11 13	-35	-11 19
-1	9	-5 -11	4	-5 -5	-1	-5 1	-6	-5 7	-11	-5 13	-16	-5 19
0	-2	1 -11	-1	1 -5	0	1 1	1	1 7	2	1 13	3	1 19
1	-13	7 -11	-6	7 -5	1	7 1	8	7 7	15	7 13	22	7 19
2	-24	13 -11	-11	13 -5	2	13 1	15	13 7	28	13 13	41	13 19
3	-35	19 -11	-16	19 -5	3	19 1	22	19 7	41	19 13	60	19 19
4	-46	25 -11	-21	25 -5	4	25 1	29	25 7	54	25 13	79	25 19

Table 4-6: "Additive x Additive PC Multiplication Chart in PC Key Values"

Columns in Tables 4-4 and 4-5 have magnitude reflected in PC Key Column 0, with sign not reflected

Rows in Tables 4-4 and 4-6 have magnitude reflected in PC Key Row 0, with sign not reflected

Both Rows and Columns are reflected between Tables 4-5 and 4-6, resulting in a 180° rotation around the intersection of PC Key Row 0 and Column 0

Calculating the PC Key value at the intersection of Row R with Column C, $K^{\pm,\pm}(R,C)=K$ at (R,C)

We shall extend the PC Key function $K(r)$ st

$K^{\pm,\pm}(R,C)=K$ at the intersection of Row R and Column C

in a table of Subtractive (-) or Additive (+) PC Rows multiplied by Columns of Subtractive (-) or Additive (+) PCs

Examining Table 4-4

$$K^{-,+}(0, C) = -C$$

$$\begin{aligned}
K^{-,+}(R, 0) &= R \\
K^{-,+}(R, C) &= R + (C * P_R^{-}) \\
&= -C + (R * P_C^{+})
\end{aligned}$$

Examining Table 4-5

$$\begin{aligned}
K^{-,-}(0, C) &= -C \\
K^{-,-}(R, 0) &= -R \\
K^{-,-}(R, C) &= -R + (C * P_R^{-}) \\
&= -C + (R * P_C^{-})
\end{aligned}$$

Examining Table 4-6

$$\begin{aligned}
K^{+,+}(0, C) &= C \\
K^{+,+}(R, 0) &= R \\
K^{+,+}(R, C) &= R + (C * P_R^{+}) \\
&= C + (R * P_C^{+})
\end{aligned}$$

Calculating the PC Key value for PC Multiples

Now that we've seen the above charts we shall examine the PC Key value of PC multiples

Case 1: Products of Subtractive PCs

$$\begin{aligned}
(6n-1) \times (6m-1) &= 6^2nm - 6n - 6m + 1 \\
&= 6(6nm - n - m) + 1
\end{aligned}$$

This is the Additive PC at PC Key Value $6nm - n - m$

$$\begin{aligned}
(6n-1) \times (6m-1) \times (6q-1) &= (6^2nm - 6n - 6m + 1) \times (6q-1) \\
&= 6^3nmq - 6^2nq - 6^2mq + 6q - 6^2nm + 6n + 6m - 1 \\
&= 6(6^2nmq - 6(nm + nq + mq) + n + m + q) - 1
\end{aligned}$$

This is the Subtractive PC at PC Key Value $6^2nmq - 6(nm + nq + mq) + n + m + q$

$$\begin{aligned}
(6n-1) \times (6m-1) \times (6q-1) \times (6r-1) \\
&= (6^3nmq - 6^2(nm + nq + mq) + 6(n + m + q) - 1) \times (6r-1) \\
&= 6^4nmqr - 6^3(nmr + nqr + mqr) + 6^2(nr + mr + qr) - 6r \\
&\quad - 6^3nmq + 6^2(nm + nq + mq) - 6(n + m + q) + 1 \\
&= 6 \{ 6^3nmqr - 6^2(nmr + nqr + mqr + nmq) \\
&\quad + 6(nr + mr + qr + nm + nq + mq) - (n + m + q + r) \} + 1
\end{aligned}$$

This is the Additive PC at PC Key Value

$$6^3nmqr - 6^2(nmr + nqr + mqr + nmq) + 6(nr + mr + qr + nm + nq + mq) - (n + m + q + r)$$

$$K((6n-1)) = n$$

$$K((6n-1) \times (6m-1)) = 6nm - n - m$$

$$K((6n-1) \times (6m-1) \times (6q-1)) = 6^2nmq - 6(nm + nq + mq) + n + m + q$$

$$K((6n-1) \times (6m-1) \times (6q-1) \times (6r-1))$$

$$\begin{aligned}
&= 6^3nmqr - 6^2(nmr + nqr + mqr + nmq) \\
&\quad + 6(nr + mr + qr + nm + nq + mq) - (n + m + q + r)
\end{aligned}$$

$$\text{Let } Q = \prod_1^m (6n_i - 1)$$

$$K(Q) = \sum_1^m (-1)^{(m-i)} x 6^{(i-1)} x \{ E_i(n_1, n_2, \dots, n_m) \}$$

where $E_i(n_1, n_2, \dots, n_m)$ is the sum of each of the permutations of products of i terms selected from m terms, without repetition. The number of products summed by $E_i(n_1, n_2, \dots, n_m)$ for a particular i

and m is the binomial coefficient $\binom{m}{i}$, ie,

$$E_3(n_1, n_2, n_3, n_4) = n_1 \cdot n_2 \cdot n_3 + n_1 \cdot n_2 \cdot n_4 + n_1 \cdot n_3 \cdot n_4 + n_2 \cdot n_3 \cdot n_4$$

Q is an Additive PC for m even, and Subtractive for m odd

Restricting ourselves to Powers of $6n-1$

$$K(6n-1) = n$$

$$K(6n-1)^2 = 6n^2 - 2n$$

$$K(6n-1)^3 = 6^2 n^3 - 3(6n^2 + n)$$

$$\begin{aligned} (6n-1)^4 &= (6(6n^2 - 2n) + 1) \times (6(6n^2 - 2n) + 1) \\ &= 6^2(6n^2 - 2n)^2 + 2 \times 6(6n^2 - 2n) + 1 \\ &= 6(6(6n^2 - 2n)^2 + 2(6n^2 - 2n)) + 1 \end{aligned}$$

Note that this PC Key Value appears to be a polynomial of the form $6x^2 + 2x$, where $x = 6n^2 - 2n = K(6n-1)^2$, which resembles the derivative of $2x^3 + x^2$

$$\begin{aligned} K(6n-1)^4 &= 6(6n^2 - 2n)^2 + 2(6n^2 - 2n) \\ &= 6^3 n^4 - 6^2 4n^3 + 6^2 n^2 - 4n, \text{ from Product formula for } Q, \text{ above} \end{aligned}$$

Case 2: Products of Additive PCs

$$\begin{aligned} (6n+1) \times (6m+1) &= 6^2 nm + 6n + 6m + 1 \\ &= 6(6nm + n + m) + 1 \end{aligned}$$

This is the Additive PC at PC Key Value $6nm + n + m$

$$\begin{aligned} (6n+1) \times (6m+1) \times (6q+1) &= (6^2 nm + 6n + 6m + 1) \times (6q+1) \\ &= 6^3 nmq + 6^2 nq + 6^2 mq + 6q + 6^2 nm + 6n + 6m + 1 \\ &= 6(6^2 nmq + 6(nm + nq + mq) + n + m + q) + 1 \end{aligned}$$

This is the Subtractive PC at PC Key Value $6^2 nmq + 6(nm + nq + mq) + n + m + q$

$$\begin{aligned} (6n+1) \times (6m+1) \times (6q+1) \times (6r+1) &= (6^3 nmq + 6^2(nm + nq + mq) + 6(n + m + q) + 1) \times (6r+1) \\ &= 6^4 nmqr + 6^3(nmr + nqr + mqr) + 6^2(nr + mr + qr) + 6r \\ &\quad + 6^3 nmq + 6^2(nm + nq + mq) + 6(n + m + q) + 1 \\ &= 6 \{ 6^3 nmqr + 6^2(nmr + nqr + mqr + nmq) \\ &\quad + 6(nr + mr + qr + nm + nq + mq) + (n + m + q + r) \} + 1 \end{aligned}$$

This is the Additive PC at PC Key Value

$$6^3 nmqr + 6^2(nmr + nqr + mqr + nmq) + 6(nr + mr + qr + nm + nq + mq) + (n + m + q + r)$$

$$\begin{aligned}
\mathbf{K}((6n + 1)) &= n \\
\mathbf{K}((6n + 1)x(6m+1)) &= 6nm + n + m \\
\mathbf{K}((6n + 1)x(6m+1)x(6q + 1)) &= 6^2nmq + 6(nm + nq + mq) + n + m + q \\
\mathbf{K}((6n + 1)x(6m+1)x(6q + 1)x(6r + 1)) \\
&= 6^3nmqr + 6^2(nmr + nqr + mqr + nmq) \\
&\quad + 6(nr + mr + qr + nm + nq + mq) + (n + m + q + r)
\end{aligned}$$

$$\text{Let } Q = \prod_{i=1}^m (6n_i + 1)$$

$$\mathbf{K}(Q) = \sum_{i=1}^m (6^{(i-1)} x \{ E_i(n_1, n_2, \dots, n_m) \})$$

where $E_i(n_1, n_2, \dots, n_m)$ is as defined for Case 1.

Note that the Additive result in \mathbf{K} is the same as for the Subtractive PCs, but with all terms positive

Q is an Additive PC for all cases

Restricting ourselves to Powers of $6n+1$

$$\begin{aligned}
\mathbf{K}((6n + 1)) &= n \\
\mathbf{K}((6n + 1)^2) &= 6n^2 + 2n \\
\mathbf{K}((6n + 1)^3) &= 6^2n^3 + 3(6n^2 + n)
\end{aligned}$$

$$\begin{aligned}
(6n + 1)^4 &= (6(6n^2 + 2n) + 1) x (6(6n^2 + 2n) + 1) \\
&= 6^2(6n^2 + 2n)^2 + 2x6(6n^2 + 2n) + 1 \\
&= 6(6(6n^2 + 2n)^2 + 2(6n^2 + 2n)) + 1
\end{aligned}$$

Note that this PC Key Value also appears to be a polynomial of the form $6x^2 + 2x$, but in this case $x = 6n^2 + 2n = \mathbf{K}((6n + 1)^2)$, which again resembles the derivative of $2x^3 + x^2$

$$\begin{aligned}
\mathbf{K}((6n + 1)^4) &= 6(6n^2 + 2n)^2 + 2(6n^2 + 2n) \\
&= 6^3n^4 + 6^24n^3 + 6^2n^2 + 4n, \text{ from Product formula for } Q, \text{ above}
\end{aligned}$$

Case 3: Subtractive by Additive PCs

$$\begin{aligned}
(6n - 1) x (6m + 1) &= 6^2nm + 6n - 6m - 1 \\
&= 6(6nm + n - m) - 1
\end{aligned}$$

This is the Subtractive PC at PC Key Value $6nm + n - m$

$$\begin{aligned}
(6n - 1) x (6m - 1) x (6q + 1) &= (6^2nm - 6n - 6m + 1) x (6q + 1) \\
&= 6^3nmq - 6^2nq - 6^2mq + 6q + 6^2nm - 6n - 6m + 1 \\
&= 6(6^2nmq + 6(nm - nq - mq) - n - m + q) + 1
\end{aligned}$$

This is the Additive PC at PC Key Value $6^2nmq + 6(nm - nq - mq) - n - m + q$

$$\begin{aligned}
(6n + 1) x (6m + 1) x (6q - 1) &= (6^2nm + 6n + 6m + 1) x (6q - 1) \\
&= 6^3nmq + 6^2nq + 6^2mq + 6q - 6^2nm - 6n - 6m - 1 \\
&= 6(6^2nmq + 6(-nm + nq + mq) - n - m + q) - 1
\end{aligned}$$

This is the Subtractive PC at PC Key Value $6^2nmq + 6(-nm + nq + mq) - n - m + q$

$$\begin{aligned}
(6n-1) \times (6m-1) \times (6q+1) \times (6r+1) &= (6^3nmq + 6^2nm - 6^2nq - 6^2mq - 6n - 6m + 6q + 1) \times (6r+1) \\
&= 6^4nmqr + 6^3nmr - 6^3nqr - 6^3mqr - 6^2nr - 6^2mr + 6^2qr + 6r \\
&\quad + 6^3nmq + 6^2nm - 6^2nq - 6^2mq - 6n - 6m + 6q + 1 \\
&= 6^4nmqr + 6^3nmq + 6^3nmr - 6^3nqr - 6^3mqr + 6^2nm - 6^2nq - 6^2mq - 6^2nr - 6^2mr + 6^2qr \\
&\quad - 6n - 6m + 6q + 6r + 1 \\
&= 6(6^3nmqr + 6^2(nmq + nmr - nqr - mqr)) + 6(nm - nq - mq - nr - mr + qr) + (-n - m + q + r) + 1 \\
&= 6(6^3nmqr + 6^2(n\{m\{q+r\} - qr\} - mqr)) + 6(n\{m - q - r\} - m\{q + r\} + qr) + (-n - m + q + r) + 1
\end{aligned}$$

This is the Additive PC at PC Key Value

$$6^3nmqr + 6^2(nmq + nmr - nqr - mqr) + 6(nm - nq - mq - nr - mr + qr) + (-n - m + q + r)$$

$$\mathbf{K}((6n \pm 1)) = n$$

$$\mathbf{K}((6n-1) \times (6m+1)) = 6nm + n - m$$

$$\mathbf{K}((6n-1) \times (6m-1) \times (6q+1)) = 6^2nmq + 6nm - 6nq - 6mq - n - m + q$$

$$\mathbf{K}((6n+1) \times (6m+1) \times (6q-1)) = 6^2nmq - 6nm + 6nq + 6mq - n - m + q$$

$$\mathbf{K}((6n-1) \times (6m-1) \times (6q+1) \times (6r+1))$$

$$= 6^3nmqr + 6^2(nmq + nmr - nqr - mqr) + 6(nm - nq - mq - nr - mr + qr) + (-n - m + q + r)$$

$$= 6^3nmqr + 6^2(n\{m\{q+r\} - qr\} - mqr) + 6(n\{m - q - r\} - m\{q + r\} + qr) + (-n - m + q + r)$$

Section 5: Generalised Prime Lattice Structures

In the spring of 1972 a chance encounter between Hugh Montgomery and Freeman Dyson lead to the discovery of the similarity between “...the distribution function for the differences between the non-trivial zeroes of Riemann's Zeta function...” and “...the form factor for the pair correlation of eigenvalues of random Hermitian matrices...” [Derbyshire, 2004].

Given the simplicity of the Prime structure I wondered whether what is really occurring here is not a strong direct relationship between the Prime structure and Physics, but is instead some sort of generic exclusion principle. The Prime Lattice structure itself may be thought of as a kind of exclusion structure with Primes only able to occur in the Lattice gaps, and the exclusion principle would be the Weave of the Prime Lattice. Structures with some form of indirect “gaps” forming the points of interest may demonstrate such similarities.

I considered, “what is it about the Prime structure which gives us Primes ?” Is it that 2×3 “exhausts” the products ? What would happen if, in some form of maths, 2×2 is greater than 4, making 4 a “Prime” ? On further consideration it is clear that the underlying property of the Prime structure itself is in the term “ ± 1 ”

Definition: The Generalised Prime Lattice Structure

$$\begin{aligned} \mathbf{B}(z) &= \{0\} \vee \{\pm P_i^{e_i}, \pm P_j^{e_j}, \dots, \pm P_k^{e_k}\}, \\ \mathbf{S}(z) &= zn - 1, \\ \mathbf{A}(z) &= zn + 1, \quad z, n \in \mathbb{Z}, z \geq 0, \end{aligned}$$

If $\mathbf{B}(\{z\}) = \{0\}$ then

$$z = 0$$

else

$$z = P_i^{e_i} \cdot P_j^{e_j} \cdot \dots \cdot P_k^{e_k}$$

where $\mathbf{B}(z)$ is the “Prime Base” for this set, and $\mathbf{B}(z)$ may be written using the product, ie $\mathbf{B}(6)$, or as a set of primes, ie $\mathbf{B}(\{\pm 2, \pm 3\})$ or $\mathbf{B}(\{2, 3\})$. ± 1 is an element of all Generalised Prime Candidate sets, $zn \pm 1$. It is the result of the cases with z and/or n equal to zero.

The X Base Primes in $\mathbf{B}(z) = \{0\} \vee \{\pm P_i^{e_i}, \pm P_j^{e_j}, \dots, \pm P_k^{e_k}\}$, if any, are the first X Primes in $\mathbf{B}(z)$ in order of size. Note that these “Base Primes in $\mathbf{B}(z)$ ” are the set $\{\pm P_i^{e_i}, \pm P_j^{e_j}, \dots, \pm P_k^{e_k}\}$, and not the set $\{\pm P_i^1, \pm P_j^1, \dots, \pm P_k^1\}$, unless $e_i = 1$ for all i , ie, the Base Primes of $\mathbf{B}(245) = \mathbf{B}(\{5, 49\})$ are 5 and 49

Prime P_{X+i} is the i^{th} prime in $\mathbf{B}(z)$ following P_X , ie, it is the $X+i^{\text{th}}$ prime in $\mathbf{B}(z)$

The Primorial of P_{X+i} in $\mathbf{B}(z)$ is $P_{z, X+i\#} = z \cdot P_{X+1} \cdot P_{X+2} \cdot \dots \cdot P_{X+i}$. I will retain $P_{X+i\#}$ as an alternative shorthand nomenclature equivalent to “ $P_{z, X+i\#}$ in the current Prime Base under consideration

I now term Primes of the form $6n \pm 1$, the “Natural Primes”, or $\mathbf{B}(6) = \mathbf{B}(2, 3) = \mathbf{B}(\pm 2, \pm 3)$, with the set of Base Primes $\{\pm 2, \pm 3\}$. In the Fundamental Theorem of Primes the Prime Base was labelled as $\mathbf{B} = \{\pm 2, \pm 3\}$. I will retain \mathbf{B} as indicating the special case of the Prime Base of the Natural Primes

The set of Prime Candidates under $\mathbf{B}(z)$, $\{zn \pm 1\}$, is closed under multiplication

$$(z n - 1) \times (z m - 1) = z^2 nm - zn - zm + 1 = z (znm - n - m) + 1$$

$$(z n - 1) \times (z m + 1) = z^2 nm + zn - zm - 1 = z (znm + n - m) - 1$$

$$(z n + 1) \times (z m + 1) = z^2 nm + zn + zm + 1 = z (znm + n + m) + 1$$

Note these are generalised forms of the multiplicative equations for the Natural Primes, with z in place of 6

$$(6n - 1) \times (6m - 1) = 6^2 nm - 6n - 6m + 1 = 6 (6nm - n - m) + 1$$

$$(6n - 1) \times (6m + 1) = 6^2 nm + 6n - 6m - 1 = 6 (6nm + n - m) - 1$$

$$(6n + 1) \times (6m + 1) = 6^2 nm + 6n + 6m + 1 = 6 (6nm + n + m) + 1$$

$\{zn \pm 1\}$ is also closed under division, with sub-factors of form $zn \pm 1$ or is itself “Prime in $\mathbf{B}(\{z\})$ ”, meaning that it does not decompose into sub-factors of form $zn \pm 1$ other than its own (+)ve or (-)ve value and ± 1

The PC Key function $\mathbf{K}(x)$ is now extended to $\mathbf{K}_z(x)$, “the value of n in $zn \pm 1$ under $\mathbf{B}(z)$ ”. I will retain $\mathbf{K}(x)$ as an alternative shorthand nomenclature equivalent to “ $\mathbf{K}_z(x)$ in the current Prime Base under consideration”

The Inverse PC Key function $\mathbf{P}^\pm(x)$ is extended to $\mathbf{P}_z^\pm(x)$. Similarly, I will retain $\mathbf{P}^\pm(x)$ as an alternative shorthand nomenclature equivalent to “ $\mathbf{P}_z^\pm(x)$ in the current Prime Base under consideration”. I shall also use

$$1) \quad \mathbf{P}^+(x) = z \lfloor x \rfloor + 1, \quad x \in \mathbb{R}, x \geq 0$$

$$2) \quad \mathbf{P}^-(x) = z \lfloor x \rfloor - 1, \quad x \in \mathbb{R}, x \geq 0$$

$$1) \quad \mathbf{P}^+(x) = z \lceil x \rceil + 1, \quad x \in \mathbb{R}^-$$

$$2) \quad \mathbf{P}^-(x) = z \lceil x \rceil - 1, \quad x \in \mathbb{R}^-$$

With $\mathbf{B}(z)$, we are not studying all integers; instead we are investigating the Patterns of the Prime Lattice structures formed over the subsets of Subtractive and Additive Prime Candidates under $\mathbf{B}(z)$, $\{zn \pm 1\}$. Theorem 11 is a corollary to Theorem 9, providing a definition for “Prime PCs in $\mathbf{B}(z)$ ”

Theorem 11: Prime PCs in $\mathbf{B}(z)$

$x = zn \pm 1$ is a Prime PC in $\mathbf{B}(z)$ iff it is not the product of a smaller Prime Candidate in $\mathbf{B}(z)$, $x' = zm \pm 1$, $\forall z, n, m \in \mathbb{Z}, z > 0, 0 < |m| < |n|$

$P_{z,i}$ is the i^{th} Prime in $\mathbf{B}(z)$. The first Primes in $\mathbf{B}(z)$ are the prime factors of z . The subsequent $\mathbf{B}(z)$ Primes are $\mathbf{B}(z)$ Prime PCs. I will retain P_i as an alternative shorthand nomenclature equivalent to “the i^{th} Prime in the current Prime Base under consideration”, ie, in $\mathbf{B}(10)$,

$$P_1=2, P_2=5, P_3=9, P_4=11, \dots$$

Similarly, I will retain P_i^\pm as alternative shorthand nomenclature equivalent to “the Subtractive, and Additive, Prime Candidates with PC Integer Key i , in the current Prime Base under consideration”, ie, in $\mathbf{B}(10)$, $P_2^- = 19, P_2^+ = 21$

There are neither Prime, nor Composite, PCs in $\mathbf{B}(0)$ as it only has the 2 PCs, ± 1

All of $B(1)$'s Primes are the same as $B(6)$'s Primes, but in $B(1)$:

- There are no Primes in the Prime Base, $B(1) = \{\pm 1\}$
- ± 2 and ± 3 are Prime PCs, not Base Primes
- All Primes are both Subtractive and Additive PCs

y is a Prime PC in $B(y - 1)$ and $B(y + 1)$ for all Integers $y, y > 1$

“ $B(z)$ Prime PC” is an equivalent term to “Prime PC in $B(z)$ ”

For example, not counting “1”, the first few (+)ve Prime PCs in $B(10)$ are:

9, 11, 19, 21, 29, 31, 39, 41, 49, 51, 59, 61, 69, 71, 79, 89, 91, 101, 109, 111, 119, 129, ...

Many $B(10)$ Prime PCs are not Natural Primes, ie not Prime in $B(6)$:

9, 21, 39, 49, 51, 69, 91, 111, 119, 129, ...

Many $B(10)$ Prime PCs are not even Prime Candidates in $B(6)$; they are of the form $x = 3(2k+1)$

9, 21, 39, 51, 69, 111, 129, ...

The first few “Composite Prime Candidates in $B(10)$ ” are:

81 = 9x9
 99 = 9x11
 121 = 11x11
 171 = 9x19
 189 = 9x21
 209 = 11x19
 231 = 11x21
 261 = 9x29

$10n-1$	$10n$	$10n+1$
...
-21	$-(2 \times 5) \times 2$	-19
-11	$-(2 \times 5)$	-9
-1	0	1
9	2x5	11
19	$2 \times 5 \times 2$	21
29	$2 \times 5 \times 3$	31
39	$2 \times 5 \times 4$	41
49	$2 \times 5 \times 5$	51
59	$2 \times 5 \times 6$	61
69	$2 \times 5 \times 7$	71
79	$2 \times 5 \times 8$	9x9
89	$2 \times 5 \times 9$	91
9x11	$2 \times 5 \times 10$	101
109	$2 \times 5 \times 11$	111
119	$2 \times 5 \times 12$	11x11
129	$2 \times 5 \times 13$	131
139	$2 \times 5 \times 14$	141
149	$2 \times 5 \times 15$	151
159	$2 \times 5 \times 16$	161
169	$2 \times 5 \times 17$	9x19
179	$2 \times 5 \times 18$	181
9x21	$2 \times 5 \times 19$	191
199	$2 \times 5 \times 20$	201

11x19	2x5x21	211
219	2x5x22	221
229	2x5x23	11x21
...
889	2x5x89	9x9x11
...

There are 15 (+)ve Prime PCs in $B(10)$ before the first $B(10)$ Composite PC, 81 { $K_{10}(81)=8$ }, then 2 more $B(10)$ Prime PCs before the next Composite $B(10)$ PC, 99 { $K_{10}(99)=10$ }, totaling 17 $B(10)$ Prime PCs below 99

There are 7 (+)ve Prime PCs in the Natural Primes, $B(6)$ { 5, 7, 11, 13, 17, 19, 23 } before the first Composite PC, 25 { $K(25)=4$ }, then 2 more Primes before the next Composite PC, 35 { $K(35)=6$ }

Thus, the “Weave” of the Prime Lattice varies depending on the value of “z”. Examining the composites formed by set of Prime Candidates under $B(z)$, { $zn \pm 1$ }:

$$K_z((z n - 1) \times (z m - 1)) = znm - n - m$$

$$K_z((z n - 1) \times (z m + 1)) = znm + n - m$$

$$K_z((z n + 1) \times (z m + 1)) = znm + n + m$$

Many of the properties documented in this paper hold for $B(z)$, ie Factorisation Algorithms in $B(z)$, there will be a Prime Number Theorem applicable to each $B(z)$, $z > 0$

For small values of n, or m, the above multiples are affected more by the value of z. As $zn \pm 1$ tends towards infinity the effect of z decreases and, for $z > 6$, the Density of Primes in Prime Candidates under $B(z)$ decreases for the same reason, and in the same manner, as the density of Primes in the Prime Candidates of the Natural Primes, $B(6)$

I also suspect that there might be secondary effects in the weave for $B(z)$ when z is a multiple of 6

Theorem 12: Infinity of “Prime PCs in $B(z)$ ”:

There are an infinite number of Prime PCs in $B(z)$, $z > 0$

Proof, by Induction:

Let $B(z)$, $z > 0$, be the Prime Structure under consideration

Add 1 to the product of z with n Primes, P_a, P_b, \dots, P_c , under $B(z)$, st no primes appear more than once, ie $a < b \forall n$ elements

$$\text{Let } Q = z \cdot (P_a \cdot P_b \cdot \dots \cdot P_c) + 1$$

$$Q \text{ is a } B(z) \text{ Prime Candidate, with PC Key } (P_a \cdot P_b \cdot \dots \cdot P_c)$$

$$Q \bmod P_i \equiv (P_i + 1) \bmod P_i \equiv 1 \bmod P_i \quad \forall P_i \in \{P_a, P_b, \dots, P_c\}$$

The factors of Q are Prime Candidates. As Q is not divisible by the n Primes, P_a, P_b, \dots, P_c , there must be a Prime PC P_d , st $P_d | Q$, $P_d \notin \{P_a, P_b, \dots, P_c\}$

Thus, there is always an $n+1^{\text{th}}$ Prime PC

Considering the product of this new set of $n+1$ primes, $P_a, P_b, \dots, P_c, P_d$

$$\text{Let } Q' = z \cdot (P_a \cdot P_b \cdot \dots \cdot P_c \cdot P_d) + 1$$

Q' is a $\mathbf{B}(z)$ Prime Candidate, with PC Key $(P_a \cdot P_b \cdot \dots \cdot P_c \cdot P_d)$

$$Q' \bmod P_i \equiv (P_i + 1) \bmod P_i \equiv 1 \bmod P_i \quad \forall P_i \in \{P_a, P_b, \dots, P_c, P_d\}$$

As Q' is not divisible by the $n+1$ Primes, $P_a, P_b, \dots, P_c, P_d$, there must be a Prime PC P_e ,
 st $P_e | Q'$, $P_e \notin \{P_a, P_b, \dots, P_c, P_d\}$

Thus, there is always an $n+2^{\text{th}}$ Prime PC

By the Principle of Mathematical Induction, $\forall n$, the existence of n Primes implies an $n+1^{\text{th}}$ Prime PC

Therefore the number of Prime PCs in $\mathbf{B}(z)$ is Infinite

If $Q=P_d$ then Q is Prime in $\mathbf{B}(z)$

If $Q'=P_e$ then Q' is Prime in $\mathbf{B}(z)$

Lattice Structures over \mathbb{R}

The domain of z in $\mathbf{B}(z)$ may be extended in at least two ways to include the Real numbers.

Case 1: Extend the Domain of the “ z ” term to \mathbb{R}

In this extended domain the Real Prime Base, $\mathbf{B}(r)$, has an infinite number of members, r^n , all of the integer powers of the Real number r

$$\begin{aligned} \mathbf{B}(z) &= \{r^n\}, \\ \mathbf{S}(z) &= r^n - 1, \\ \mathbf{A}(z) &= r^n + 1, \quad n \in \mathbb{Z}, r \in \mathbb{R}, r \geq 0, \end{aligned}$$

Case 2: Extend the Domain of n to \mathbb{R}

Another way to extend the domain into the Reals is to extend n into the Reals instead of z . This subset is formed by taking a Real number, r_0 , and all of the Reals an integer displacement from r_0

$$n = \{r_0 + y\}, r_0 \in \mathbb{R}, y \in \mathbb{Z}$$

Then

$$\begin{aligned} \mathbf{B}(z) &= \{0\} \vee \{\pm P_i^{e_i}, \pm P_j^{e_j}, \dots, \pm P_k^{e_k}\}, \\ \mathbf{S}(z) &= z \{r_0 + y\} - 1, \\ \mathbf{A}(z) &= z \{r_0 + y\} + 1, \quad z \in \mathbb{Z}, z \geq 0, r_0 \in \mathbb{R}, y \in \mathbb{Z} \end{aligned}$$

I have not had the opportunity to research these two extended domains. I believe their structures to also be lattices, but with sub-lattices spawned between every integer. These sub lattices then decrease in value. I am also interested in investigating the possibility that these two structures may directly map to each other

Lattice Structures over \mathbb{C}

A Gaussian Integer is a Complex number $z=a+bi$, where a and b are integers. Gaussian Integers can be uniquely factored in terms of Gaussian Primes [Weisstein (3)]

A Gaussian Prime is a Gaussian Integer which is only divisible by itself and 1, and by no other

Gaussian Integer. [Loy (1)]

Definition: Gaussian primes are Gaussian integers satisfying one of the following properties [Weisstein (4)].

1. If both a and b are nonzero then $a+bi$ is a Gaussian prime iff $a^2 + b^2$ is a Natural Prime.
2. If $a = 0$, then bi is a Gaussian prime iff $|b|$ is a Natural Prime and $b \equiv 3 \pmod{4}$.
3. If $b = 0$, then a is a Gaussian prime iff $|a|$ is a Natural Prime and $a \equiv 3 \pmod{4}$.

The Natural Primes which are also Gaussian Primes are 3, 7, 11, 19, 23, 31, 43, ... [Sloane A002145]. 2 is a Natural prime, but it is not a Gaussian prime because it has Gaussian Integer factors,

$$(1 - i)(1 + i) = 1 + 1 = 2$$

Theorem 13: A Prime Candidate Structure of Gaussian Primes

For Gaussian Prime $z = a+bi$. If $a = 0$, or $b = 0$, then if $|z| > 3$ and the Integer Key Value, $n = K(|z|)$ is:

- Even, then $|z|$ is a Subtractive Prime, $6n - 1, n > 1$,
- Odd, then $|z|$ is an Additive Prime, $6n + 1, n > 0$,

Proof:

$$z = a + bi$$

If $a=0$ then $|z|=|b|$. If $b=0$ then $|z|=|a|$

From points 2 and 3 of the definition of Gaussian Primes,

$|z|$ is a Natural Prime > 0 and $z \equiv 3 \pmod{4}$

$$|z| = 6n \pm 1, n \geq 0$$

$$= (4+2)n \pm 1$$

$$= 4n + 2n \pm 1$$

If $n=0$ then $|z|=1$ which is not congruent to 3 (mod 4)

Therefore $n > 0$

If $|z|$'s Integer Key Value $n = K(|z|)$ is even, ie $n = 2k, k \geq 0$, then

$$|z| = 4(2k) + 2 \cdot 2k \pm 1$$

$$\equiv 0 \pmod{4} \pm 1 \text{ for Gaussian Primes}$$

$$\equiv 3 \pmod{4} \text{ only for Subtractive Primes, with } n > 1$$

If $|z|$'s Integer Key Value, $K(|z|) = n$, is odd, ie $n = 2k + 1, k \geq 0$, then

$$a = 4(2k + 1) + 2 \cdot (2k + 1) \pm 1$$

$$= 4(2k + 1) + 2 \cdot 2k + 2 \pm 1$$

$$\equiv 0 \pmod{4} + 2 \pm 1$$

$$\equiv 3 \pmod{4} \text{ only for Additive Primes, with } n > 0$$

Note that Theorem 13 only describes the structure of a subset of the Gaussian Primes. There may be more Prime Candidate, or other, types of structures to consider.

Section 6: Generalising Euclid's Proof of the Infinitude of Primes

aka: How the Prime Structure was discovered

In this Section, we examine General Forms of Euclid's Proof of the Infinitude of Primes, and how they lead to the discovery of the underlying structure of Primes.

For the sake of clarity refer Appendix A for proofs using these General Forms.

Euclid's Theorem: *There are an infinite number of Primes*

From Euclid's Proof of the Infinitude of Primes, *cf Appendix A:Proof 1*, the equation

$$(1.1) \quad Q = \prod_{i=1}^n P_i + 1$$

can be used to prove that there are an infinite number of Primes, as Q is indivisible by P_i for all $i = 1$ to n . Thus \exists prime P_k where $P_k | Q$, st $P_k \neq P_i \quad \forall i, i=1$ to $n, P_n < P_k \leq Q, n < k$

If $Q = P_k$ then Q is Prime

It holds from equation 1.1 that:

$$(1.2) \quad Q \bmod P_n \# \equiv 1 \bmod P_n \#$$

$$(1.3) \quad Q \bmod P_i \equiv (P_i + 1) \bmod P_i \equiv 1 \bmod P_i \quad \forall P_i, 1 \leq i \leq n$$

which also imply that there is a $n+1^{\text{th}}$ Prime

It follows that the Corollary equation

$$(2.1) \quad Q' = P_n \# - 1, n \geq 1$$

can also be used to prove that there are an infinite number of Primes, *refer Appendix A:Proof 2*, on the grounds that Q' is indivisible by P_i for all $i = 1$ to n , ie

$$(2.2) \quad Q' \bmod P_n \# \equiv (P_n \# - 1) \bmod P_n \# \equiv -1 \bmod P_n \#$$

$$(2.3) \quad Q' \bmod P_i \equiv (P_i - 1) \bmod P_i \equiv -1 \bmod P_i \quad \forall P_i, 1 \leq i \leq n$$

For the purpose of clarity, we shall work with an abbreviated notation for the General Forms of Euclid's Proof and its Corollary, always taking care to note the respective use of “+” and “-” terms

Equations 1.1 and 2.1 generalise to the abbreviated form, Equation 3, *refer Appendix A:Proof 3*

$$(3) \text{ Let } Q^{\pm} = P_n \# \pm 1, 1 \leq n$$

Substitute “ P_{n+1} ” for “1” in Equation 3

$$(4) \quad Q^{\pm} = P_n \# \pm P_{n+1}, 1 \leq n$$

As Q^{\pm} is not divisible by P_2, \dots, P_n, P_{n+1} , then Equation 4 $\Rightarrow \exists$ Primes P_j, P_k , st $P_j | Q^-, P_k | Q^+, P_{n+1} < P_j, P_k, n+1 < j, k$

Substituting “ $P_m \# / P_n \#$ ” for “ P_{n+1} ” in Equation 4.1

$$(5.1) \quad Q^{\pm} = P_n \# \pm \frac{P_m \#}{P_n \#}, \quad 1 \leq n \leq m$$

$$\Rightarrow \exists \text{ Primes } P_j, P_k, \text{ st } P_j | Q^-, P_k | Q^+, P_m < P_j, P_k, m < j, k$$

In practice Equation 5.1 appears to be a Prime Number Pair Generator, returning both (+)ve and (-)ve Primes. On further investigation this may be found to fail for some input domains, if so, I feel that there may yet be restrictions applicable to the input domain which would generate an infinite range of Primes.

As an aside, Equation 5.1 can be restricted to positive Primes,

$$(5.2) \quad Q^{\pm} = \left| P_n \# \pm \frac{P_m \#}{P_n \#} \right|, \quad 1 \leq n \leq m$$

Another aside, if $m=n$ then equation 5.1 collapses to Equation 3

$$(5.3) \quad Q^{\pm} = P_n \# \pm \frac{P_n \#}{P_n \#} = P_n \# \pm 1, \quad 1 \leq n = m$$

It was not until after preliminary release of this paper that I discovered $13\# + 1 = 30,031 = 59 \times 509$

Then, for $i=1$ to n , include primes P_i as factors to either the LHS or RHS term of Equation 5.2, but not both,

$$(6) \quad Q^{\pm} = \prod_i^n P_i^{E_i} \pm \prod_i^n P_i^{(1-E_i)}, \quad E_i \in \{0,1\}, \quad 1 \leq n$$

$$\Rightarrow \exists \text{ Primes } P_j, P_k, \text{ st } P_j | Q^-, P_k | Q^+, P_n < P_j, P_k, n < j, k$$

Note: Equation 3 is a Special Case of Equation 6, with $E_i = 1 \quad \forall i \geq 1$

While we can continue to generalise the equations, Equation 6 does not generate only Primes

$$Q^{\pm} = 2^1 \cdot 3^1 \cdot 5^1 \cdot 7^0 \cdot 11^1 \pm 2^0 \cdot 3^0 \cdot 5^0 \cdot 7^1 \cdot 11^0$$

$$= 330 \pm 7$$

$$= \{323, 337\}$$

$$= \{\text{Composite} (=17 \times 19), \text{Prime}\}$$

If we then raise primes P_i to the powers, m_i ,

$$(7) \quad Q^{\pm} = \prod_i^n P_i^{m_i E_i} \pm \prod_i^n P_i^{m_i (1-E_i)}, \quad 0 < m_i, m_i \in \mathbb{Z}, E_i \in \{0,1\}, \quad 1 \leq n$$

$$\Rightarrow \exists \text{ Primes } P_j, P_k, \text{ st } P_j | Q^-, P_k | Q^+, P_n < P_j, P_k, n < j, k$$

Equation 7 also generates Composites

$$Q^{\pm} = 2^2 \cdot 3^1 \cdot 5^1 \cdot 7^0 \cdot 11^1 \pm 2^0 \cdot 3^0 \cdot 5^0 \cdot 7^1 \cdot 11^0$$

$$= 660 \pm 7$$

$$= \{653, 667\}$$

$$= \{\text{Prime}, \text{Composite} (=23 \times 29)\}$$

Allow m_i to equal 0

$$(8) \quad Q^{\pm} = \prod_i^n P_i^{m_i E_i} \pm \prod_i^n P_i^{m_i (1-E_i)}, \quad 0 \leq m_i, m_i \in \mathbb{Z}, E_i \in \{0,1\}, \quad 1 \leq n$$

$$\Rightarrow \exists \text{ Primes } P_j, P_k, \text{ st } P_j | Q^-, P_k | Q^+, P_n < P_j, P_k, n < j, k$$

Equation 8 has a side-effect in that, in some cases, it is a factorisation algorithm in reverse. This is because m_i may equal 0, for some i , which therefore effectively removes prime P_i from the equation.

Prime P_i may then become a factor of Q^\pm

$$\begin{aligned} Q^\pm &= 2^0 \cdot 3^0 \cdot 5^1 \cdot 7^1 \cdot 11^0 \pm 2^0 \cdot 3^0 \cdot 5^0 \cdot 7^0 \cdot 11^1 \\ &= 35 \pm 11 \\ &= \{24, 46\} \\ &= \{Composite (=2^3 \times 3), Composite (=2 \times 23)\} \end{aligned}$$

All primes appeared to have solutions satisfying the form of Equation 8, but Equation 8 also generates Composites

At this stage of my investigations I lacked sufficient knowledge of the Primes to prove the conditions under which Equations 1.1 through 5.1 may generate only Primes and was unaware of the existence of the Lattice Structure.

Given the Hypothesis that Equation 5.1 is a Prime Number Generator, or may have restricted input which generates an infinite range of Primes, why does scrambling the same primes over both the Left and Right hand terms generate both Primes and Composites in Equation 6 ?

It was my attempts to answer this question which lead to the discovery of the structure of Primes. Due to software limitations, and pen and paper, I was mostly working with small primes as the domain, ie $P_i=2$ to 11. This work had the numbers 2 through 11 swapping sides in equations 5.1 and 6. I also noticed that separating 2 and 3 between the left and right hand terms within equation 6 could generate Composites as well as Primes. This lead me from Equation 6 to Equations 7 and 8

$$\begin{aligned} &= 2^1 \cdot 3^0 \cdot 5^1 \cdot 7^1 \cdot 11^1 \cdot 13^0 \pm 2^0 \cdot 3^1 \cdot 5^0 \cdot 7^0 \cdot 11^0 \cdot 13^1 \\ &= 770 \pm 39 \\ &= \{731, 809\} \\ &= \{Composite (=17 \times 43), Prime\} \end{aligned}$$

Expressing Equation 5.1 in Function Set Notation, and including $P_0^\pm=1$ in our domain

$$(9.1) \quad \rho(m, n) = Q^\pm = P_n \# \pm \frac{P_m \#}{P_n \#}, \quad 0 \leq n \leq m$$

$$(9.2) \quad \rho(m, n) = \left\{ P_n \# + \frac{P_m \#}{P_n \#}, P_n \# - \frac{P_m \#}{P_n \#} \right\}, \quad 0 \leq n \leq m$$

When considering a single parameter, m , define $\rho(m)$ as the set collecting $\rho(m, n)$

$$(9.3) \quad \rho(m) = \{ \{ \rho(m, m) \}, \{ \rho(m, m-1) \}, \dots, \{ \rho(m, 1) \} \}, \quad 0 \leq n \leq m$$

Results of Equation 9.3

$\rho(0)$	2	0												
$\rho(1)$	3	1	3	-1										
$\rho(2)$	7	5	5	-1	7	-5								
$\rho(3)$	31	29	11	1	17	-13	31	-29						
$\rho(4)$	211	209	37	23	41	-29	107	-103	211	-209				
$\rho(5)$	2311	2309	221	199	107	-47	391	-379	1157	-1153	2311	-2309		
$\rho(6)$	30031	30029	2323	2297	353	67	1031	-971	5011	-4999	15017	-15013	30031	-30029

Due to my interest in products of 2 and 3 I noticed that there were relationships with multiples of 6

$\rho(0)$	2	0												
$\rho(1)$	3	6.0+1												
$\rho(2)$	6+1	6-1	6-1	6.0-1	6.1+1	-6.1+1								
$\rho(3)$	6.5+1	6.5-1	6.2-1	1	6.3-1	-6.2-1	6.5+1	-6.5+1						
$\rho(4)$	6.35+1	6.35-1	6.6+1	6.4-1	6.7-1	-6.5+1	6.18-1	-6*17-1	6.35+1	-6.35+1				
$\rho(5)$	6.385+1	6.385-1	6.37-1	6.33+1	6.18-1	-6.8+1	6*65+1	-6.63-1	6.193-1	-6.192-1	6.385+1	-6.385+1		
$\rho(6)$	6.5005+1	6.5005-1	6.387+1	6.383-1	6*59-1	6.11+1	6.172-1	-6.162+1	6.835+1	-6.833-1	6.2503-1	-6.2502-1	6.5005+1	-6.5005+1

Note:

$$\rho(0,0) = \{\text{Prime} = 2, \text{Composite} = 0\}$$

Midway point of $\rho(m, m)^+$ and $\rho(m, m)^- = 2 \times \text{midway point of } \rho(m, 1)^+ \text{ and } |\rho(m, 1)^-|, m > 1$

ie, $6n = 2 \cdot (3n)$, for some n

$$\rho(m, m) = 6n \pm 1, \quad \rho(m, 1) = 2 \pm 3n, \quad \rho(m, 0) = 1 \pm 6n \text{ for } m > 1$$

$$\rho(m, 2) = 6 \pm n, \rho(m, 3) = 6.5 \pm n/5$$

From here it was clear that a sampled range of small Primes, other than 2 and 3, appeared to be of the form

$$(9.4) \quad \rho(m, n) = Q^{\pm} = 6 \frac{P_n \#}{P_2 \#} \pm \frac{P_m \#}{P_n \#}, \quad 2 \leq n \leq m$$

$$(9.5) \quad \rho(m, m) = Q^{\pm} = 6 \frac{P_m \#}{P_2 \#} \pm 1, \quad 2 \leq m$$

At this stage I went to the Internet to check what was known about “6n” and “Primes”

I found a number of websites with proofs that all primes greater than 3 are of the form $6n \pm 1$ [Caldwell] [Hui] [Loy (2)]. I realised that it was actually the case that all primes OTHER than 2 and 3 are of the form $6n \pm 1$; as I was considering both “1” and negative integers as Prime solutions to my Equations.

I asked myself “what about the $6n \pm 1$ numbers that aren't Prime ?”

To answer that question I drew up *Table 1-1: “Integers modulo 6”* and discovered the structure underlying Prime numbers

I then proceeded to document this research into Generalising Euclid's Proof. I realised that the Prime structure could also be separately derived from First Principles. I felt that would be a clearer approach for presenting this research and moved this section on Generalising Euclid's Proof towards the end of this paper.

At this stage I am right back where I started from before I discovered the Prime Lattice. I am still left with the unproven Hypothesis of *Symmetric Primes*; which many will recognise is actually a generalised form of the Twin Primes Hypothesis.

Hypothesis 1: Symmetric Primes

$$\rho(m, n) = P_n \# \pm \frac{P_m \#}{P_n \#}, \quad 1 \leq n \leq m, \quad n, m \in \mathbb{Z}$$

generates an infinite number of Primes, an infinite subset of which are pairs of Primes symmetric about $P_n \#$

Some of the results of $\rho(m, n)$ which are not Prime.

$2\# - 1 = 1$	Neither Prime nor Composite
$3\# - 5 = 1$	Neither Prime nor Composite
$13\# + 1 = 30,031 = 59 \times 509$	Composite

Thus, Hypothesis 1 was the original form of Prime Structure which I generalised to Hypothesis 2 and finally simplified to the Fundamental Theorem of Primes and the Prime Lattice structure

Hypothesis 2: Symmetric Prime Structure

All Natural Primes may be expressed in the form

$$Q^{\pm} = -1^m \cdot \left(\prod_i^n P_i^{E_i} \pm \prod_i^n P_i^{(1-E_i)} \right), \quad m, E_i \in \{0, 1\}, \quad 1 \leq n, n \in \mathbb{Z}$$

cf Hypothesis 2 with Equation 6, above, or Appendix A: Proof 6 of Euclid's Theorem

Hypotheses 1 and 2 are generalised logical steps from Theorems 3 and 4 in the same nature of exhausting all Primes, and exhaust the missing displacements of Theorem 6 as Theorem 6 was restricted to a displacement of ± 1 .

For the purposes of clarity we shall ignore the factor of -1^m , for the moment

$$n=1, Q^\pm = 1, 3, -1, 3$$

$$n=2, Q^\pm = 5, 7, 1, 5, -1, 5, -5, 7$$

$$n=3,$$

	LHS	RHS	Q^-	Q^+
	30	1	29	31
	15	2	13	17
	10	3	7	13
	6	5	1	11
	5	6	-1	11
	3	10	-7	13
	2	15	-13	17
	1	30	-29	31

$$n=4,$$

	LHS	RHS	Q^-	Q^+
	210	1	209	211
	105	2	103	107
	70	3	67	73
	42	5	37	47
	30	7	23	37
	35	6	29	41
	21	10	11	31
	14	15	-1	29
	15	14	1	29
	10	21	-11	31
	6	35	-29	41
	7	30	-23	37
	5	42	-37	47
	3	70	-67	73
	2	105	-103	107
	1	210	-209	211

Note that the Binomial equation controls the results of this equation

Hypothesis 3: Symmetric Primes in $B(z)$

$$\rho_z(m, n) = P_n \# \pm \frac{P_m \#}{P_n \#}, \quad X \leq n \leq m, \quad n, m \in \mathbb{Z}, \quad X \text{ is the number of Base Primes } \in B(z)$$

generates an infinite number of $B(z)$ Primes, an infinite subset of which are pairs of $B(z)$ Primes symmetric about $P_n \#$

Hypothesis 4: Symmetric Integers

All Integers may be expressed in the form

$$Q^{\pm} = \prod_i^n P_i^{m_i E_i} \pm \prod_i^n P_i^{m_i (1-E_i)}, \quad 0 \leq m_i, \quad m_i \in \mathbb{Z}, \quad E_i \in \{0,1\}, \quad 1 \leq n$$

Section 7: Symmetric Prime Lattices

In this Section, we examine Symmetric Prime Lattices, refer *Figure 7-1: "Symmetries of $\{6n \pm 1\}$ over $[-31, 343]$ ".* and state an hypothesis in terms of Prime Lattice theory which is equivalent to the Symmetric Primes Hypothesis

It appears that the validity of the Symmetric Primes Hypothesis is dependent on the weave of the Prime Structure and the resultant location of the Prime Holes.

Figure 7-1 shows that every pattern of Composite strands has a cycle of length "6 x Product of the strands" and 180° Rotational Symmetry repeated at half of this cycle length, starting from 0 K. ie, a pair of Composite strands $z_i=6n_i-1$ and $z_j=6n_j+1$ have a cycle of length $6n_i n_j$, or $n_i n_j$ K, and repeated 180° Rotational Symmetry at every $3n_i n_j$, $= (n_i n_j)/2$ K, starting from 0 K. The cycle and symmetry length properties hold regardless of the number of strands involved.

The Symmetries shown in Figure 7-1 were discovered as part of this investigation. The weave "pattern" of these symmetries still hold when transformed by a factor of 6.

In Figure 7-1, from left to right, the graphs are Composite strands of:

<i>Strand(s)</i>	<i>Cycle Length</i>	<i>Points of Symmetry</i>
13	13 K	6.5n K
25	25 K	12.5n K
5, 7	35 K (=6x35 =210)	17.5n K (=3x35n =105n)
5,11	55 K	27.5n K
5,13	65 K	32.5n K
7,11	77 K	38.5n K
5,17	85 K	42.5n K
7,13	91 K	45.5n K
7,17	119 K	59.5n K
7,19	133 K	66.5n K
11,13	143 K	71.5n K
5,7,11	385 K	192.5n K
17,19,23,25	185,725 K	92,862.5n K

Table 7-1: "Symmetries of $\{6n \pm 1\}$ "

$n \in \mathbb{Z}$

These symmetries hold for all $B(z)$, for Integer values of z , with z being the size of unit K. I have not investigated these symmetries yet in terms of Real z

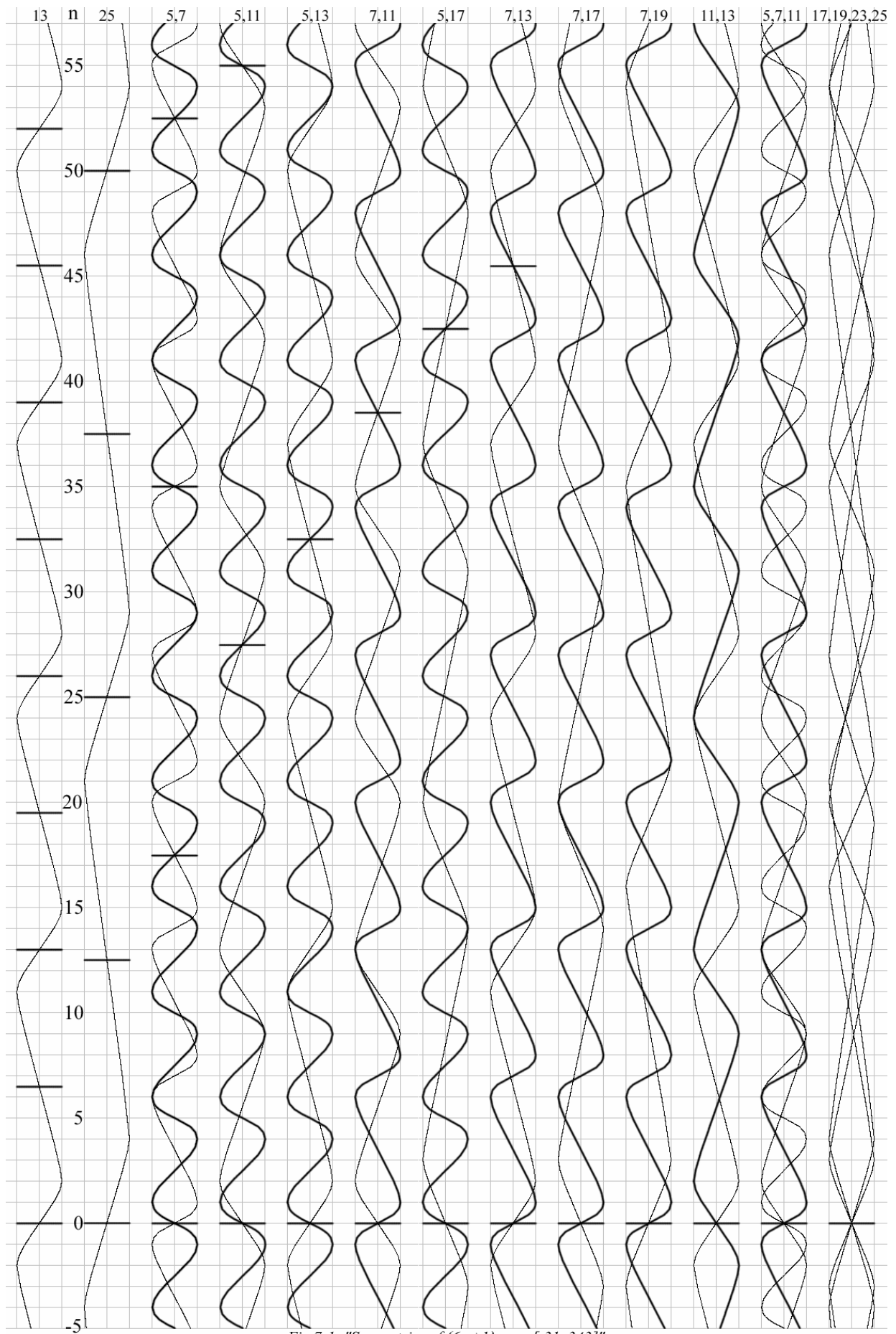


Fig 7-1: "Symmetries of $\{6n \pm 1\}$ over $[-31, 343]$ "

Expressing the Symmetric Primes Hypothesis in terms of Prime Lattice Theory

$$\rho(m, n) = 6 \frac{P_n\#}{P_2\#} \pm \frac{P_m\#}{P_n\#}, \quad 2 \leq n \leq m$$

$$\rho(m, n) = P_n\# \pm \prod_{i=n+1}^m P_i, \quad 2 \leq n \leq m$$

$\rho(m, n)$ is a Prime PC distance from $P_n\#$ only when $m=n+1$

1) If $m=n$ then $\rho(m, n) = P_n\# + 1$, 1 is a PC, but considered neither Prime nor Composite

2) If $m=n+1$ then $\rho(m, n) = P_n\# + P_{n+1}$, a Prime PC displacement from $P_n\#$

3) If $m > n+1$ then $\rho(m, n) = P_n\# \pm \prod_{i=n+1}^m P_i$, a Composite Prime Candidate displacement

of P_d^\pm , where $P_d^\pm = \prod_{i=n+1}^m P_i$

The Symmetric Primes Hypothesis is equivalent to transforming every Prime Candidate strand by a factor of 6 and then adding or subtracting Prime Candidate multiples, resulting in Prime Candidates. An infinite number of these resulting Prime Candidates will themselves be Primes, and an infinite number of these Prime PCs will form pairs of Primes symmetric about the point of displacement, $P_n\#$

Equivalently: There exist an infinite number of $\rho(m, n)$ st

$$P_j \nmid (P_n\# \pm P_m\#/P_n\#), \quad \text{for all } P_j \text{ st } P_n < P_j < (P_n\# \pm P_m\#/P_n\#)$$

Due to P_d^\pm having a sliding symmetrical cycle of length $6P_d^\pm = P_d^\pm K$, the effect of this displacement on the shape of the strand of P_d^\pm is to displace the shape by only $P_n\# \bmod 6P_d^\pm$

Thus we are left with an open hypothesis which is a restatement of the Symmetric Primes Hypothesis in terms of the Prime Lattice Structure and, if proved, would also prove the Symmetric Primes Hypothesis

Appendix A: General Forms of Euclid's Proof of the Infinitude of Primes
Euclid's Theorem: There are an infinite number of Primes

Definition: P_i is the i^{th} Prime, $P_1=2, P_2=3, P_3=5, P_4=7, \dots$

Proof 1a of Euclid's Theorem, by Contradiction:

Assume there are only n Primes. Add 1 to the product of all n primes

$$(1a.1) \text{ Let } Q = \prod_{i=1}^n P_i + 1$$

$$(1a.2) \quad Q \bmod P_n \equiv 1 \bmod P_n$$

$$(1a.3) \quad Q \bmod P_i \equiv (P_i + 1) \bmod P_i \equiv 1 \bmod P_i \quad \forall P_i, 1 \leq i \leq n$$

As $Q > 1$ and not divisible by the Primes P_1, \dots, P_n , there must be a Prime P_k , st $P_k | Q, P_n < P_k \leq Q, n < k$

Thus, there is always an $n+1^{\text{th}}$ Prime

Contradiction

Therefore the number of Primes is Infinite

If $Q = P_k$ then Q is Prime

Proof 1b of Euclid's Theorem, by Induction:

Add 1 to the product of n primes, P_a, P_b, \dots, P_c , st no primes appear more than once, ie $a < b \forall n$ elements

$$(1b.1) \text{ Let } Q = (P_a \cdot P_b \cdot \dots \cdot P_c) + 1$$

$$(1b.2) \quad Q \bmod P_i \equiv (P_i + 1) \bmod P_i \equiv 1 \bmod P_i \quad \forall P_i \in \{P_a, P_b, \dots, P_c\}$$

As Q is not divisible by the n Primes, P_a, P_b, \dots, P_c , there must be a Prime P_d ,
 st $P_d | Q, P_d \notin \{P_a, P_b, \dots, P_c\}$

Thus, there is always an $n+1^{\text{th}}$ Prime

By considering the product of this new set of $n+1$ primes, $P_a, P_b, \dots, P_c, P_d$

$$(1b.3) \text{ Let } Q' = (P_a \cdot P_b \cdot \dots \cdot P_c \cdot P_d) + 1$$

$$(1b.4) \quad Q' \bmod P_i \equiv (P_i + 1) \bmod P_i \equiv 1 \bmod P_i \quad \forall P_i \in \{P_a, P_b, \dots, P_c, P_d\}$$

As Q' is not divisible by the $n+1$ Primes, $P_a, P_b, \dots, P_c, P_d$, there must be a Prime P_e ,
 st $P_e | Q', P_e \notin \{P_a, P_b, \dots, P_c, P_d\}$

Thus, there is always an $n+2$ th Prime

By the Principle of Mathematical Induction, $\forall n$, the existence of n Primes implies an $n+1$ th Prime
Therefore the number of Primes is Infinite

If $Q=P_d$ then Q is Prime
If $Q'=P_e$ then Q' is Prime

Corollary to Proof 1 - Proof 2 of Euclid's Theorem:

Assume there are only n Primes, $n \geq 1$. Subtract 1 from the product of all n primes

$$(2.1) \text{ Let } Q' = P_n \# - 1$$

As Q' is not divisible by the Primes P_1, P_2, \dots, P_n , there must be a Prime P_j , st $P_j | Q'$, $P_n < P_j \leq Q'$, $n < j$

Thus, there is always an $n+1$ th Prime
Contradiction
Therefore the number of Primes is Infinite

If $Q'=P_j$ then Q' is Prime

It also holds from equation 2.1 that:

$$(2.2) \quad Q' \bmod P_n \# \equiv (P_n \# - 1) \bmod P_n \# \equiv -1 \bmod P_n \#$$

$$(2.3) \quad Q' \bmod P_i \equiv (P_i - 1) \bmod P_i \equiv -1 \bmod P_i \quad \forall P_i, 1 \leq i \leq n$$

Lemma 1

Let P be Prime, then $\gcd(P, a) = |P|$ or 1 &

$$(P, a) = 1 \text{ iff } P \nmid a$$

$$(P, a) = |P| \text{ iff } P | a$$

Each of 2.2 and 2.3 also show that there must be a Prime P_j , st $P_j | Q'$, $P_n < P_j \leq Q'$, $n < j$

Abbreviated Form: The First Generalised Form of the Euclidean Proof:

As per Section 1 of this paper, for the purpose of brevity, we shall work with an abbreviated notation for Euclid's Proof and its Corollary, always taking care to note the respective use of “+” and “-” terms

Proof 3 of Euclid's Theorem - Proofs 1 and 2 combined:

Assume there are only n Primes, $n \geq 1$. Add $\{Q^+\}$, or subtract $\{Q^-\}$, 1 to the product of all n primes

$$(3.1) \text{ Let } Q^{\pm} = P_n \# \pm 1$$

As Q^- and Q^+ are not divisible by the Primes P_1, P_2, \dots, P_n , there must be Primes P_j, P_k st $P_j|Q^-, P_k|Q^+, P_n < P_j, P_n < P_k, n < j, n < k$

$$\text{GCD}(P_j, P_k) = 1$$

Thus, there is always an $n+1$ th Prime. If $n \geq 2$ then there is also always an $n+2$ th Prime
 Contradiction
 Therefore the number of Primes is Infinite

If $Q^- = P_j$ then Q^- is Prime. If $Q^+ = P_k$ then Q^+ is Prime.

It also holds from equation 3.1 that:

$$(3.2) \quad Q^\pm \pmod{P_n \#} \equiv (P_n \# \pm 1) \pmod{P_n \#} \equiv \pm 1 \pmod{P_n \#}$$

$$(3.3) \quad Q^\pm \pmod{P_i} \equiv (P_i \pm 1) \pmod{P_i} \equiv \pm 1 \pmod{P_i} \quad \forall P_i, 1 \leq i \leq n$$

Proof 4 of Euclid's Theorem:

(Substituting " P_{n+1} " for "1" in Equation 3.1)

WLOG, assume there are only $n+1$ Primes. Add, or subtract, prime P_{n+1} to the product of all n primes

$$(4.1) \quad \text{Let } Q^\pm = P_n \# \pm P_{n+1}$$

As Q^\pm is not divisible by $P_1, P_2, \dots, P_n, P_{n+1}$ (4.1) $\Rightarrow \exists$ Primes P_j, P_k , st $P_j|Q^-, P_k|Q^+, P_j, P_k > P_{n+1}, j, k > n+1$

Thus, there is always an $n+1$ th Prime. If $n \geq 2$ then there is also always an $n+2$ th Prime
 Contradiction
 Therefore the number of Primes is Infinite

If $Q^- = P_j$ then Q^- is Prime. If $Q^+ = P_k$ then Q^+ is Prime.

It also holds from equation 4.1 that:

$$(4.2) \quad Q^\pm \pmod{P_n \#} \equiv (P_n \# \pm P_{n+1}) \pmod{P_n \#} \equiv \pm P_{n+1} \pmod{P_n \#} \neq 0$$

$$(4.3) \quad Q^\pm \pmod{P_i} \equiv (P_i \pm P_{n+1}) \pmod{P_i} \equiv \pm P_{n+1} \pmod{P_i} \neq 0 \quad \forall P_i, 1 \leq i \leq n$$

Proof 5 of Euclid's Theorem:

(Substituting " $P_{n+m} \# / P_n \#$ " for " P_{n+1} " in Equation 4.1)

WLOG, assume there are only $n+m$ Primes. Add, or subtract, prime " $P_{n+m} \# / P_n \#$ " to the product of all n primes

$$(5.1) \quad Q^{\pm} = P_n \# \pm \frac{P_{n+m} \#}{P_n \#}, m \geq 0$$

$$\Rightarrow \exists \text{ Primes } P_j, P_k, \text{ st } P_j | Q^-, P_k | Q^+, \\ P_{n+m} < P_j, P_{n+m} < P_k, n+m < j, n+m < k$$

Thus, there is always an $n+1$ th Prime. If $n \geq 2$ then there is also always an $n+2$ th Prime
 Contradiction
 Therefore the number of Primes is Infinite

Proof 6 of Euclid's Theorem:

Assume there are only n Primes, $n \geq 1$. Then, $\forall i, i=1$ to n , include primes P_i as factors to either the LHS or RHS term, but not both, ie

$$(6) \quad Q^{\pm} = \prod_i^n P_i^{E_i} \pm \prod_i^n P_i^{(1-E_i)}, E_i \in \{0, 1\}$$

$$\Rightarrow \exists \text{ Primes } P_j, P_k, \text{ st } P_j | Q^-, P_k | Q^+, \\ P_n < P_j, P_n < P_k, n < j, n < k$$

Thus, there is always an $n+1$ th Prime. If $n \geq 2$ then there is also always an $n+2$ th Prime
 Contradiction
 Therefore the number of Primes is Infinite

Proof 7 of Euclid's Theorem:

Assume there are only n Primes. $\forall i, i=1$ to n , include exponents, m_i , of primes P_i as factors to either the LHS or RHS term, but not both, ie

$$(7) \quad Q = \prod_i^n P_i^{m_i E_i} \pm \prod_i^n P_i^{m_i (1-E_i)}, m_i > 0, m_i \in \mathbb{Z}, E_i \in \{0, 1\}$$

$$\Rightarrow \exists \text{ Primes } P_j, P_k, \text{ st } P_j | Q^-, P_k | Q^+, \\ P_n < P_j, P_n < P_k, n < j, n < k$$

Thus, there is always an $n+1$ th and an $n+2$ th Prime
 Contradiction
 Therefore the number of Primes is Infinite

Appendix B: Factorisation Algorithms

```
solna=398075086424064937397125500550386491199064362342526708406385189575946388957261768583317
solnb=472772146107435302536223071973048224632914695302097116459852171130520711256363590397527
```

```
print "soln A is Additive (6n+1) = "
(solna-1) % 6
print "soln B is Subtractive (6n-1) = "
(solnb+1) % 6
print "soln A - soln B = "
solna-solnb
print "soln B - soln A = "
solnb-solna
print "\n"
```

```
z=188198812920607963838697239461650439807163563379417382700763356422988859715234665485319060606
504743045317388011303396716199692321205734031879550656996221305168759307650257059
print "z = \n"
z
```

```
print "length(z)="
length(z)
```

```
print "\n"
print "z mod 6 = "
z%6
print "z mod 3 = "
z%3
print "z mod 2 = "
z%2
```

```
print "\n"
c=z+1
print "(z+1) mod 6 = "
print c%6
print " [ <== Should be 0]\n\n"
```

```
sqrtz=sqrt(z)
print "sqrt(z) = "
sqrtz
print "z-(sqrt(z)^2) = "
z-(sqrtz*sqrtz)
print "z-({sqrt(z)+1}^2) = "
print z-((sqrtz+1)*(sqrtz+1))
print " [ <== Should be (-)ve]\n\n"
```

```
sqrt6c=sqrt(c)
print "sqrt(6c) = "
sqrt6c
print "(z+1)-(sqrt(6c)^2) = "
(z+1)-(sqrt6c*sqrt6c)
print "(z+1)-({sqrt(6c)+1}^2) = "
print (z+1)-((sqrt6c+1)*(sqrt6c+1))
print " [ <== Should be (-)ve]\n\n"
```

```
c=c/6
print "c = (z+1) / 6 = "
c
```

```

sqrtc=sqrt(c)
print "sqrt(c) = "
sqrtc
print "c-(sqrt(c)^2) = "
c-(sqrtc*sqrtc)
print "c-({sqrt(c)+1}^2) = "
print c-((sqrtc+1)*(sqrtc+1))
print " [ <== Should be (-)ve]\n\n"

```

```

sqrtcon6=sqrt(c/6)
print "sqrt(c/6) = "
sqrtcon6
print "(c/6)-(sqrt(c/6)^2) = "
(c/6)-(sqrtcon6*sqrtcon6)
print "(c/6)-({sqrt(c/6)+1}^2) = "
print (c/6)-((sqrtcon6+1)*(sqrtcon6+1))
print " [ <== Should be (-)ve]\n\n"

```

```

print "(6*sqrtc-1)-solna="
(6*sqrtc-1)-solna
print "(6*sqrtcon6-1)-solna="
(6*sqrtcon6-1)-solna
print "(6*sqrtcon6-1)-solnb="
(6*sqrtcon6-1)-solnb

```

D:>bc RSA_576.txt

bc 1.06

Copyright 1991-1994, 1997, 1998, 2000 Free Software Foundation, Inc.

This is free software with ABSOLUTELY NO WARRANTY.

For details type `warranty'.

soln A is Additive $(6n+1) = 0$

soln B is Subtractive $(6n-1) = 0$

soln A - soln B = -7469705968337036513909757142266173343385033295957\

0408053466981554574322299101821814210

soln B - soln A = 74697059683370365139097571422661733433850332959570\

408053466981554574322299101821814210

z =

18819881292060796383869723946165043980716356337941738270076335642298\

88597152346654853190606065047430453173880113033967161996923212057340\

31879550656996221305168759307650257059

length(z)=174

z mod 6 = 5

z mod 3 = 2

z mod 2 = 1

$(z+1) \bmod 6 = 0$ [<== Should be 0]

sqrt(z) = 4338188710978442023896232853369682906054694563015589302934\

45695571862781832679867424802

z-(sqrt(z)^2) = 3514425664418662733196236564715131185886733761648047\

90573372343299501858924404525517855

z-({sqrt(z)+1}^2) = -51619517575382213145962291420242346262226553643\

8313070013519047844223704740955209331750 [<== Should be (-)ve]

sqrt(6c) = 433818871097844202389623285336968290605469456301558930293\

```

445695571862781832679867424802
(z+1)-(sqrt(6c)^2) = 35144256644186627331962365647151311858867337616\
4804790573372343299501858924404525517856
(z+1)-({sqrt(6c)+1}^2) = -51619517575382213145962291420242346262265\
536438313070013519047844223704740955209331749 [ <== Should be (-)\
ve]

c = (z+1) / 6 = 3136646882010132730644953991027507330119392722990289\
71167938927371648099525391109142198434344174571742195646685505661193\
66615386867622338646591776166036884194793217941709510
sqrt(c) = 1771058124966578484160094122632612707348581868347683836848\
02725764108106372034872588743
c-(sqrt(c)^2) = 2712168873721387478805842713511528336589052596988024\
53610468934629160556555579531389461
c-({sqrt(c)+1}^2) = -82994737621176948951434553175369707810811113970\
734313759136516899055656188490213788026 [ <== Should be (-)\
ve]

sqrt(c/6) = 72303145182974033731603880889494715100911576050259821715\
574282595310463638779977904133
(c/6)-(sqrt(c/6)^2) = 1061664870895727747899058316435349845397896951\
82702117581137164107622336488495651803229
(c/6)-({sqrt(c/6)+1}^2) = -38439803276375292673301930135454445662033\
456917817525850011401082998590789064304005038 [ <== Should be (-)\
ve]

(6*sqrtc-1)-solna=66455978855588215309893097302918113321008475866608\
3593702431165008702249274947466949140
(6*sqrtcon6-1)-solna=35743784673779264992497784786581799406405093959\
032221887060505995916392875418098841480
(6*sqrtcon6-1)-solnb=-3895327500959110014659978663607993402744523900\
0538186166406475558657929423683722972730
quit

```

References:

Caldwell, Chris K., "Are all primes (past 2 and 3) of the forms $6n+1$ and $6n-1$?"
<http://www.utm.edu/research/primes/notes/faq/six.html>

Derbyshire, John, 2003, *Prime Obsession*. ISBN: 0452285259
Chapter 18

Hoffman, Paul, 1998, *The Man Who Loved Only Numbers*. ISBN:1-85702-811-2
1) P92 - "...Erdős was the master of elementary methods..."
2) P32-33 – Euclid's Proof of the Infinitude of Primes

Hui, K., "Infinitely many Primes of form $6n+5$ ".
<http://nrich.maths.org/askedNRICH/edited/3640.html>

Ingham, A. E., 1932, *The Distribution of Prime Numbers*. ISBN: 0-521-39789-8

Jameson, G. J. O., 2003, *The Prime Number Theorem*. ISBN: 0-521-89110-8

Loy, J, (1) "Gaussian Primes".
<http://www.jimloy.com/algebra/gprimes.htm>

Loy, J, (2) "Primes and 6".
<http://www.jimloy.com/number/prime6.htm>

RSA, "RSA Challenge".
<http://www.rsasecurity.com/rsalabs/node.asp?id=2093>

Sloane A002145
<http://www.research.att.com/cgi-bin/access.cgi/as/njas/sequences/eisA.cgi?Anum=A002145>

Weisstein, Eric W. (1) "Fundamental Theorem of Arithmetic." From MathWorld--A Wolfram Web Resource. <http://mathworld.wolfram.com/FundamentalTheoremofArithmetic.html>

Weisstein, Eric W. (2) "Prime Number Theorem." From MathWorld--A Wolfram Web Resource. <http://mathworld.wolfram.com/PrimeNumberTheorem.html>

Weisstein, Eric W. (3) "Gaussian Integer." From MathWorld--A Wolfram Web Resource. <http://mathworld.wolfram.com/GaussianInteger.html>

Weisstein, Eric W. (4) "Gaussian Prime." From MathWorld--A Wolfram Web Resource. <http://mathworld.wolfram.com/GaussianPrime.html>