The Curious Reluctance to Define Prime Probability Non-Heuristically

Bhupinder Singh Anand

The Curious Reluctance to Define Prime Probability *Non-Heuristically*

&

An elementary probability-based approach to estimating prime counting functions *non-heuristically*

Bhupinder Singh Anand

Draft of September 15, 2015

Abstract. The reluctance to define the probability of a number being prime *non-heuristically* is curious, since we can define the residues $i > r_i(n) \geq 0$ for all $n \geq 2$ and all $i \geq 2$ such that $r_i(n) = 0$ if, and only if, i is a divisor of n, and show: (i) that $\mathbb{M}_i = \{(0, 1, 2, \ldots, i-1),\ r_i(n), \frac{1}{i}\}$ is a probability model for $r_i(n)$; and (ii) that the joint *non-heuristic* probability $\mathbb{P}(r_{p_i}(n) = 0 \ \cap \ r_{p_j}(n) = 0)$ of two primes $p_i \neq p_j$ dividing any integer n is the product $\mathbb{P}(r_{p_i}(n) = 0).\mathbb{P}(r_{p_j}(n) = 0)$. We conclude that the *non-heuristic* probability of n being a prime p is given by the *non-heuristic* prime probability function $\mathbb{P}(n \in \{p\}) = \prod_{i=1}^{\pi(\sqrt{n})}(1-\frac{1}{p_i}) \sim \frac{2e^{-\gamma}}{log_e n}$. By the Law of Large Numbers, the number $\pi(n)$ of primes less than or equal to n is therefore *non-heuristically* approximated by $\pi_{_L}(n) = \sum_{j=1}^{n}\prod_{i=1}^{\pi(\sqrt{j})}(1-\frac{1}{p_i})$. We show that, in the interval $(p_n^2,\ p_{n+1}^2)$, the *non-heuristic* approximation $\pi_{_L}(x)$ of $\pi(x)$ is a straight line with gradient $\prod_{i=1}^{n}(1-\frac{1}{p_i})$; and that the function $\pi_{_L}(x)/\frac{x}{log_e x}$ is differentiable with derivative $(\pi_{_L}(x)/\frac{x}{log_e x})' \in o(1)$. We conclude by the Law of Large Numbers that $\pi(x) \sim \pi_{_L}(x)$ since $p_{n+1}^2 - p_n^2 \to \infty$; and that both $\pi_{_L}(x)/\frac{x}{log_e x}$ and $\pi(x)/\frac{x}{log_e x}$ do not oscillate as $x \to \infty$. Chebyshev's Theorem, $\pi(x) \asymp \frac{x}{log_e x}$, then yields an elementary probability-based proof of the Prime Number Theorem $\pi(x) \sim \frac{x}{log_e x}$. We also give an elementary probability-based proof that the number $\pi_{_{(a,d)}}(n)$ of Dirichlect primes of the form $a + m.d$ which are less than or equal to n, where a, d are co-prime and $1 \leq a < d = q_1^{\alpha_1}.q_2^{\alpha_2}\ldots q_k^{\alpha_k}$ (q_i prime), is *non-heuristically* approximated by the *non-heuristic* Dirichlect prime counting function $\pi_{_D}(n) = \prod_{i=1}^{k}\frac{1}{q_i^{\alpha_i}}.\prod_{i=1}^{k}(1-\frac{1}{q_i})^{-1}.\pi_{_L}(n) \to \infty$. We finally give an elementary probability-based proof that the number $\pi_2(n)$ of twin primes $\leq n$ is approximated by the non-heuristic twin-prime counting function $\pi_{_T}(n) = \sum_{j=1}^{n}\mathbb{P}(j \in \{p\} \cap j+2 \in \{p\})$; and conclude by the Law of Large Numbers that there are infinitely many twin primes since we show that $\pi_2(n) \sim \pi_{_T}(n) \sim e^{-2\gamma}.\frac{n}{log_e^2 n}$.

Keywords. non-heuristic prime counting function; non-heuristic prime probability function; Brocard's conjecture; Chebyshev's Theorem; complete system of incongruent residues; computational complexity; Dirichlect primes; Euler's constant γ; expected value; factorising is polynomial time; Hardy-Littlewood conjecture; integer factorising algorithm; Law of Large Numbers; Mertens' theorem; mutually independent prime divisors; polynomial time algorithm; prime counting function $\pi(n)$; prime density; primes in an arithmetical progression; Prime Number Theorem; probability model; probabilistic number theory; twin primes.

2010 Mathematics Subject Classification. 11A07, 11A41, 11A51, 11N36, 11Y05, 11Y11, 11Y16

Contents

I am indebted to my erstwhile classmate, Professor Chaitanya Kumar Harilan Mehta, for his unqualified encouragement and support for my scholarly pursuits over the years; most pertinently for his patiently critical insight into, and persistent insistence upon, the required rigour for defining the probability of a number being prime *non-heuristically*, without which this extension of a 1964 investigation into the nature of divisibility and the structure of the primes—begun whilst yet classmates—would have vanished into some black hole of the informal universe of seemingly self-evident truths.

1. The curious reluctance to define prime probability *non-heuristically*

1.A. Conventional wisdom

Conventional number-theory wisdom appears to be that the distribution of primes suggested by the Prime Number Theorem, $\pi(n) \sim \frac{n}{log_e n}$, is such that the probability $\mathbb{P}(n \in \{p\})$ of an integer n being a prime p can *only* be *heuristically* estimated as $\frac{1}{log_e n}$; apparently reflecting an implicit faith in G. H. Hardy and J. E. Littlewood's 1922 dictum that[1]:

> "*Probability is not a notion of pure mathematics, but of philosophy or physics*".

It is a dictum that can reasonably be taken by the laity to suggest, with some authority, that the specific probability $\mathbb{P}(n \in \{p\})$ of an integer n being a prime p is also *not capable* of being well-defined *non-heuristically*[2] independently of the Theorem.

1.B. Defining prime divisibility *non-heuristically*

However, what intrigues about the conventional perspective of the cognoscenti is that any lay investigation of such a probability from first principles:

(1) would begin naturally by considering if, and only if, conditions for i to be a divisor of n;

(2) would move fairly straightforwardly to an elementary residue function such as $r_i(n)$[3], defined (Definition 1) for all $n \geq 2$ and all $i \geq 2$ by:

$$n + r_i(n) \equiv 0\ (mod\ i) \text{ where } i > r_i(n) \geq 0$$

since $r_i(n) = 0$ if, and only if, i is a divisor of n;

(3) would then (Theorem 2.3) note for any $i \geq 2$ that:

$$\mathbb{M}_i = \{(0, 1, 2, \ldots, i-1),\ r_i(n), \tfrac{1}{i}\}$$

[1] [Gr95], p.19, fn.16 and p.20; *see also* [HL23], fn.4 on p.37, for the origin of the quote (courtesy Prof. Andrew Granville).

[2] See, for instance, [St02], Chapter 2, p.9, Theorem (*sic*) 2.1.

[3] Depicted graphically in §4., Appendix II(A), Fig.3.

is a probability model[4] for the values of $r_i(n)$ for $n \geq 2$;

(4) which would further imply:

(i) first (Corollary 2.4) that, by the standard definition of the probability $\mathbb{P}(e)$ of an event e[5], the *non-heuristic* probability $\mathbb{P}(p|n)$ that $r_p(n) = 0$—whence the prime p divides n—is:

$$\mathbb{P}(p|n) = \tfrac{1}{p}$$

and the *non-heuristic* probability $\mathbb{P}(p \nmid n)$ that $r_p(n) \neq 0$—whence the prime p does not divide n—is:

$$\mathbb{P}(p \nmid n) = 1 - \tfrac{1}{p}$$

since the p numbers $0, 1, \ldots, (p-1)$ are all incongruent and form a complete system of residues[6];

(ii) second (Lemma 2.5) that:

(a) the product of the individual *non-heuristic* probability of $r_{p_i}(n) = 0$—whence the prime p_i divides the integer n—and the individual *non-heuristic* probability that $r_{p_j}(n) = 0$—whence the prime $p_j \neq p_i$ divides n—is:

$$\mathbb{P}(p_i|n).\mathbb{P}(p_j|n) = \tfrac{1}{p_i}.\tfrac{1}{p_j}$$

(b) the joint *non-heuristic* probability $\mathbb{P}(p_i|n \cap p_j|n)$ of $r_{p_i}(n) = 0$ *and* $r_{p_j}(n) = 0$—whence *both* the primes $p_i \neq p_j$ divide the integer n—is:

$$\mathbb{P}(p_i|n \ \cap \ p_j|n) = \tfrac{1}{p_i.p_j}$$

since the $p_i.p_j$ numbers $v.p_i + u.p_j$, where $p_i > u \geq 0$ and $p_j > v \geq 0$, are also all incongruent and form a complete system of residues[7];

(iii) and third (Theorem 2.8) that the prime divisors of any integer n are thus mutually independent by the standard definition of the 'mutual independence' of two events e_1 and e_2[8].

1.C. Defining prime probability *non-heuristically*

Now what intrigues is that, since n is a prime if, and only if, it is not divisible by any prime $p \leq \sqrt{n}$, it would immediately then follow:

(i) first (Theorem 2.11) that the *non-heuristic* probability of n being a prime p is given[9] by the *non-heuristic* prime probability function (cf. Fig.1 below):

[4] See §3., Appendix I.
[5] See §3., Appendix I; also [Ko56], Chapter I, §1, Axiom III, p.2.
[6] [HW60], p.49.
[7] Ibid., p.52, Theorem 59.
[8] See §3., Appendix I; also [Ko56], Chapter VI, §1, Definition 1, p.57 and §2, p.58; see also [Ka59], p.54.
[9] Compare [HL23], pp.36-37.

$$\mathbb{P}(n \in \{p\}) = \prod_{i=1}^{\pi(\sqrt{n})}(1 - \tfrac{1}{p_i}) \sim \tfrac{2e^{-\gamma}}{log_e n},$$

where $2.e^{-\lambda} \approx 1.12292\ldots$[10];

Fig.1: The graph of $y = \prod_{i=1}^{\pi(\sqrt{x})}(1 - \frac{1}{p_i})$

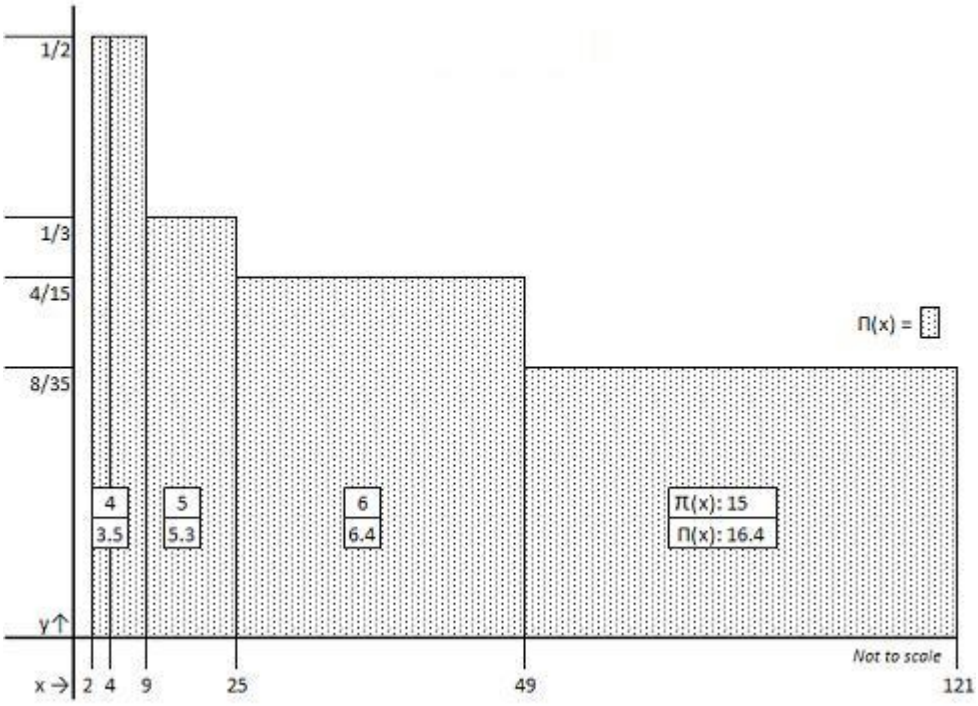

Fig.1: Graph of $y = \prod_{i=1}^{\pi(\sqrt{x})}(1 - \frac{1}{p_i})$. The dotted rectangles represent $(p_{j+1}^2 - p_j^2)\prod_{i=1}^{j}(1 - \frac{1}{p_i})$ for $j \geq 1$. Figures within boxes are values of the corresponding function within the interval $(p_j^2,\ p_{j+1}^2)$ for $j \geq 2$. The area under the curve is $\sqcap(x) = (x - p_n^2)\prod_{i=1}^{n}(1 - \frac{1}{p_i}) + \sum_{j=1}^{n-1}(p_{j+1}^2 - p_j^2)\prod_{i=1}^{j}(1 - \frac{1}{p_i}) + 2$ (see Fig.2).

(ii) and second that (Theorem 2.13), by the Law of Large Numbers[11], a *non-heuristic* estimate[12] of the number $\pi(n)$ of primes less than or equal to n is (Definition 4) the *non-heuristic* prime counting function $\pi_{_L}(n)$ (cf. Fig.2 below), such that:

$$\pi(n) \sim \pi_{_L}(n) = \sum_{j=1}^{n}\prod_{i=1}^{\pi(\sqrt{j})}(1 - \tfrac{1}{p_i}).$$

[10] [Gr95], p.13.
[11] See §3., Appendix I; also [Ko56], Chapter VI, §3, p.61.
[12] i.e. 'expected value': see §3., Apendix II. Compare also [HL23], pp.36-37.

Fig.2: The graph of $y = \sqcap(x) = \pi_{_L}(x)$

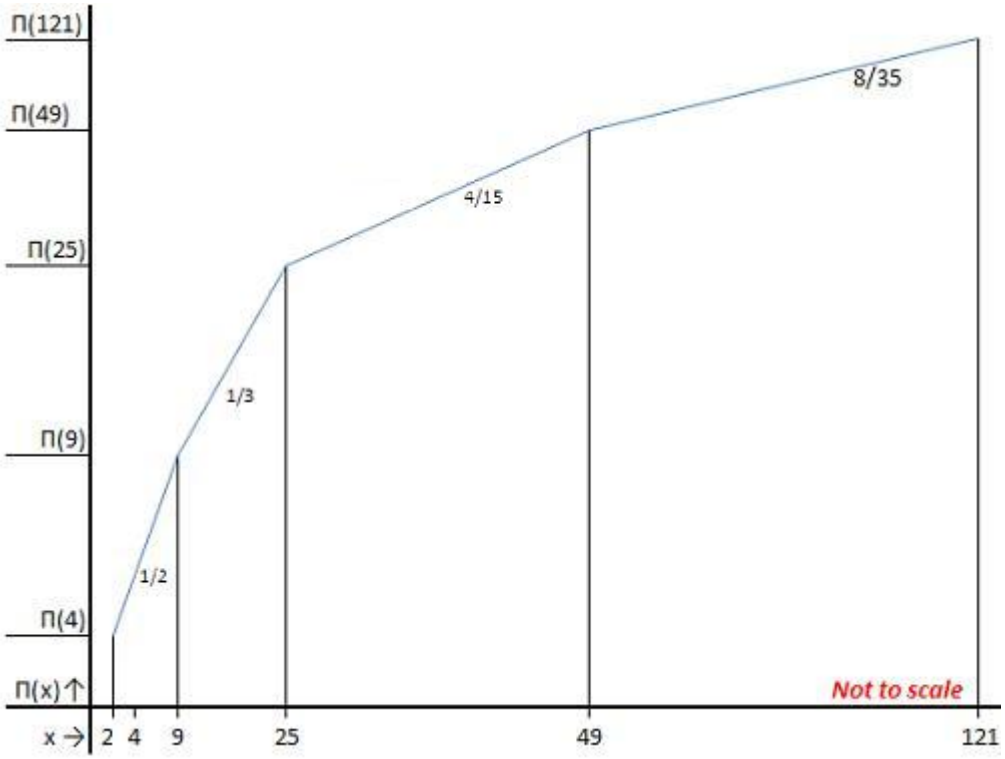

Fig.2: Graph of $y = \sqcap(x) = \pi_{_L}(x) = (x - p_n^2)\prod_{i=1}^{n}(1 - \frac{1}{p_i}) + \sum_{j=1}^{n-1}(p_{j+1}^2 - p_j^2)\prod_{i=1}^{j}(1 - \frac{1}{p_i}) + 2$ in the interval $(p_n^2,\ p_{n+1}^2)$. Note that the gradient in the interval $(p_n^2,\ p_{n+1}^2)$ is $\prod_{i=1}^{n}(1 - \frac{1}{p_i})$.

1.D. An intriguing anomaly concerning prime counting functions

However conventional number theory wisdom—whilst reasonably conceding[13] that the *heuristic* probability of an integer n being prime *could* also be naïvely assumed as $\prod_{i=1}^{\sqrt{n}}(1 - \frac{1}{p_i})$—seems to unreasonably argue against such naïvety, by concluding that the number $\pi(n)$ of primes less than or equal to n suggested by such probability would then be approximated by the *heuristic* prime counting function:

$\pi_{_H}(n) = \sum_{j=1}^{n}\prod_{i=1}^{\pi(\sqrt{n})}(1 - \frac{1}{p_i}) = n.\prod_{i=1}^{\pi(\sqrt{n})}(1 - \frac{1}{p_i}) \sim \frac{2.e^{-\gamma}n}{log_e n}$.

For instance, Hardy and Littlewood note that:

> "In the first place we observe that any formula in the theory of primes, deduced from considerations of probability, is likely to be erroneous in just this way. Consider, for example, the problem 'what is the chance that a large number n should be prime?' We know that the answer is that the chance is approximately $\frac{1}{log\ n}$.
>
> Now the chance that n should not be divisible by any prime less than a *fixed* x is asymptotically equivalent to

$$\prod_{\varpi<x}(1 - \frac{1}{\varpi})$$

[13] [Gr95], p.13.

and it would be natural to infer[1] that the chance required is asymptotically equivalent to

$$\prod_{\varpi<\sqrt{x}}(1-\frac{1}{\varpi})$$

But

$$\prod_{\varpi<\sqrt{x}}(1-\frac{1}{\varpi})\sim\frac{2e^{-C}}{log\ n}$$

and our inference is incorrect, to the extent of a factor $2e^{-C}$.

[1] One might well replace $\varpi<\sqrt{x}$ by $\varpi<x$, in which case we should obtain a probability half as large. This remark is in itself enough to show the unsatisfactory character of the argument."

. . . pp.36-37, G.H Hardy and J.E. Littlewood, *Some problems of 'partitio numerorum:' III: On the expression of a number as a sum of primes,* Acta Mathematica, December 1923, Volume 44, pp.1-70.

However, even if we ignore the incongruity of treating x as '*fixed*', the '*character*' of the argument in Hardy and Littlewood's footnoted remark can be considered '*unsatisfactory*' only if we conflate necessity with sufficiency!

Otherwise, what we ought to reasonably conclude from the argument is that:

Lemma 1.1. *Whilst the joint non-heuristic probability that n should not be divisible by any prime ϖ less than x is $\prod_{\varpi<x}(1-\frac{1}{\varpi})$ if $x\leq\sqrt{n}$, it is defined by $\prod_{\varpi<\sqrt{n}}(1-\frac{1}{\varpi})$—and not by $\prod_{\varpi<x}(1-\frac{1}{\varpi})$—if $x>\sqrt{n}$.*

Proof: We shall show in §2.A. of this investigation that whilst—if $x>\sqrt{n}$—the terms of the former product do, those of the latter product do not, *non-heuristically* define the probabilities of the necessary and sufficient—mutually independent—conditions that *jointly* define the primality of n under the probability model (see §2.B.):

- $\mathbb{M}_i=\{(0,1,2,\ldots,i-1),\ r_i(n),\frac{1}{i}\}$. □

Moreover, the argument that we may treat $\pi_{_H}(n)$ as a *heuristic* approximation to $\pi(n)$ is 'unreasonable' since an apparent anomaly does, then, surface when we express $\pi(n)$ and the function $\pi_{_H}(n)$ in terms of the number of primes determined by each function respectively in each interval $(p^2_{_n},\ p^2_{_{n+1}})$ as follows:

$$\begin{aligned}
\pi(p^2_{_{n+1}}) &= \textstyle\sum_{j=1}^{n}(\pi(p^2_{_{j+1}})-\pi(p^2_{_j}))+\pi(p^2_{_1})\\
\pi_{_H}(p^2_{_{n+1}}) &= p^2_{_{n+1}}.\textstyle\prod_{i=1}^{\pi(\sqrt{p^2_{_{n+1}}})}(1-\frac{1}{p_i})\\
&= (\textstyle\sum_{j=1}^{n}(p^2_{_{j+1}}-p^2_{_j})+p^2_{_1}).\prod_{i=1}^{n}(1-\frac{1}{p_i})\\
&= \textstyle\sum_{j=1}^{n}(p^2_{_{j+1}}.\prod_{i=1}^{n}(1-\frac{1}{p_i})-p^2_{_j}.\prod_{i=1}^{n}(1-\frac{1}{p_i}))+p^2_{_1}.\prod_{i=1}^{n}(1-\frac{1}{p_i})
\end{aligned}$$

Reason: By Corollary 2.13, $\pi_{_L}(n)$ is a *non-heuristic* estimate of $\pi(n)$, and, for any given $k>1$:

$$\pi_{_L}(p^2_{k+1}) - \pi_{_L}(p^2_k) > 0 \text{ as } n \to \infty;$$

whilst, for any given $k > 1$[14]:

$$p^2_{k+1}.\prod_{i=1}^{n}(1-\tfrac{1}{p_i}) - p^2_k.\prod_{i=1}^{n}(1-\tfrac{1}{p_i}) \to 0 \text{ as } n \to \infty.$$

More specifically, by Corollary 2.13 and Mertens' Theorem[15], the *non-heuristic* estimate of the number of primes between the prime squares p^2_k and p^2_{k+1} (see Fig.1), for any $k > 1$, is given by:

$$\begin{array}{rcl}
\pi(p^2_{k+1}) - \pi(p^2_k) & \sim & \pi_{_L}(p^2_{k+1}) - \pi_{_L}(p^2_k) \; as \; k \to \infty \\
\pi_{_L}(p^2_{k+1}) - \pi_{_L}(p^2_k) & = & (p^2_{k+1} - p^2_k).\prod_{i=1}^{k}(1-\tfrac{1}{p_i}) \\
& \geq & ((p_k+2)^2 - p^2_k).\prod_{i=1}^{k}(1-\tfrac{1}{p_i}) \\
& \geq & 4(p_k+1).\prod_{i=1}^{k}(1-\tfrac{1}{p_i}) \\
& \in & O(\tfrac{p_k}{log_e p_k}) \; as \; k \to \infty \\
& \to & \infty \; as \; k \to \infty
\end{array}$$

So, if we were to contrarily accept both $\pi_{_L}(n)$ and $\pi_{_H}(n)$ as prime counting functions, then the anomaly noted by Hardy and Littlewood would, indeed, follow from the Prime Number Theorem $\pi(n) \sim \frac{n}{log_e n}$, since $\pi_{_H}(n) \sim \frac{2.e^{-\gamma}n}{log_e n}$!

Brocard's conjecture: We note without further comment that Brocard's conjecture:

$$\pi(p^2_{k+1}) - \pi(p^2_k) \geq 4$$

would follow if we could show that, for $k > 1$, the difference between $\pi(n)$ and $\pi_{_L}(n)$ is always less than $4(p_k+1).\prod_{i=1}^{k}(1-\frac{1}{p_i}) + 1$.[16]

1.E. The 'second' Hardy-Littlewood conjecture concerning prime density

What is intriguing is that the 'heuristic' definition of the probability of a number being prime, albeit discounted by Hardy and Littlewood as 'unsatisfactory', is not only straightforwardly justifiable *non-heuristically* (as shown in §2.D.), but that Definition 4 immediately implies:

Theorem 1.2. $\pi_{_L}(m+n) \leq \pi_{_L}(m) + \pi_{_L}(n)$ *for all integers* $m, n \geq 2$

Proof: The m terms of the summation $\pi_{_L}(m) = \sum_{j=1}^{m}\prod_{i=1}^{\pi(\sqrt{j})}(1-\frac{1}{p_i})$ are identical to the first m terms of $\pi_{_L}(m+n) = \sum_{j=1}^{m+n}\prod_{i=1}^{\pi(\sqrt{j})}(1-\frac{1}{p_i})$; whilst the k^{th} term $\prod_{i=1}^{\pi(\sqrt{k})}(1-\frac{1}{p_i})$ of $\pi_{_L}(n)$ is greater than the corresponding $(m+k)^{th}$ term $\prod_{i=1}^{\pi(\sqrt{m+k})}(1-\frac{1}{p_i})$ of $\pi_{_L}(m+n)$ for $m \geq 1,\ k \geq 1$[17]. □

We further have, by the Law of Large Numbers, that:

Corollary 1.3. $\pi(m+n) \leq \pi(m) + \pi(n)$ *as* $m \to \infty$ □

The significance of Theorem 1.2 is seen if we compare:

[14] Compare with what appears to be a similar argument in [St02], Chapter 2, p.9, Theorem (*sic*) 2.1.
[15] [HW60], Theorem 429, p.351.
[16] cf. Wikipedia: Brocard's conjecture.
[17] As is graphically obvious from Fig.1.

(i) Theorem 1.2 with the definition of the 'second' Hardy-Littlewood 1923 conjecture in Richards[18] concerning the estimated density of primes as:

'$\pi(x+y) \leq \pi(x) + \pi(y)$ for all integers $x,\ y \geq 2$'

where the author claims:

"We show that this assertion is probably false";

(ii) and Corollary 1.3 with the original conjecture in [HL23][19], where Hardy and Littlewood define:

"$\varrho(x) = \overline{lim}_{n\to\infty}(\pi(n+x) - \pi(n))$"

and remark that:

> "It is plain that the determination of a lower bound for $\varrho(x)$ is a problem of exceptional depth. ... The problem of an upper bound has greater possibilities. ... An examination of the primes less than 200 suggests forcibly that: $\varrho(x) \leq \pi(x)$ $(x \geq 2)$".

2. An elementary probability-based approach to estimating prime counting functions *non-heuristically*

In the rest of this investigation we demonstrate the broader significance of defining the probability of n being a prime non-heuristically by giving elementary probability-based proofs that:

(i) *The Prime Number Theorem*: First, by the Law of Large Numbers, $\pi(x) \sim \pi_{_L}(x)$ since $p^2_{n+1} - p^2_n \to \infty$ (Corollary 2.13). Second, the function $\pi_{_L}(x)/\frac{x}{log_e x}$ is differentiable in the interval $(p^2_n,\ p^2_{n+1})$ with derivative $(\pi_{_L}(x)/\frac{x}{log_e x})' \in o(1)$ (Lemma 2.15). We conclude that both $\pi_{_L}(x)/\frac{x}{log_e x}$ and $\pi(x)/\frac{x}{log_e x}$ do not oscillate as $x \to \infty$.

Chebyshev's Theorem, $\pi(x) \asymp \frac{x}{log_e x}$, then yields the Prime Number Theorem (Theorem 2.16):

$\pi(x) \sim \frac{x}{log_e x}$.

(ii) *Dirichlect's Theorem*: By the Law of Large Numbers, the number $\pi_{(a,d)}(n)$ of Dirichlect primes of the form $a + m.d$ which are less than or equal to n, where a, d are co-prime and $1 \leq a < d = q_1^{\alpha_1}.q_2^{\alpha_2} \ldots q_k^{\alpha_k}$ (q_i prime), is approximated by the non-heuristic Dirichlect prime counting function $\pi_{_D}(n)$ (Definition 6), such that:

$\pi_{(a,d)}(n) \sim \pi_{_D}(n) = \prod_{i=1}^{k} \frac{1}{q_i^{\alpha_i}} . \prod_{i=1}^{k}(1 - \frac{1}{q_i})^{-1}.\pi_{_L}(n) \to \infty$.

(iii) *Twin Prime Theorem*: By the Law of Large Numbers, the number $\pi_2(n)$ of twin primes $\leq n$ is approximated by the non-heuristic twin-prime counting function:

[18] [Ri74], p.420.
[19] pp.52-54.

$\pi_{_T}(n) = \sum_{j=1}^{n} \mathbb{P}(j \in \{p\} \ \cap \ j+2 \in \{p\})$.

We conclude that there are infinitely many twin primes since we show that (Corollary 2.34):

$\pi_{_2}(n) \sim \pi_{_T}(n) \sim e^{-2\gamma}.\frac{n}{log_e^2 n}$.

2.A. The residues $r_i(n)$.

We begin by formally defining the residues $r_i(n)$ for all $n \geq 2$ and all $i \geq 2$ as below[20]:

Definition 1. $n + r_i(n) \equiv 0 \ (mod\ i)$ *where* $i > r_i(n) \geq 0$.

Since each residue $r_i(n)$ cycles over the i values $(i-1, i-2, \ldots, 0)$, these values are all incongruent and form a complete system of residues[21] *mod* i.

It immediately follows that:

Lemma 2.1. $r_i(n) = 0$ *if, and only if,* i *is a divisor of* n. □

2.B. The probability model $\mathbb{M}_i = \{(0, 1, 2, \ldots, i-1),\ r_i(n), \frac{1}{i}\}$

By the standard definition of the probability $\mathbb{P}(e)$ of an event e[22], we have by Lemma 2.1 that:

Lemma 2.2. *For any* $n \geq 2,\ i \geq 2$ *and any given integer* $i > u \geq 0$*:*

- *the probability* $\mathbb{P}(r_i(n) = u)$ *that* $r_i(n) = u$ *is* $\frac{1}{i}$*;*
- $\sum_{u=0}^{u=i-1} \mathbb{P}(r_i(n) = u) = 1$*;*
- *and the probability* $\mathbb{P}(r_i(n) \neq u)$ *that* $r_i(n) \neq u$ *is* $1 - \frac{1}{i}$. □

By the standard definition of a probability model[23], we conclude that:

Theorem 2.3. *For any* $i \geq 2$, $\mathbb{M}_i = \{(0, 1, 2, \ldots, i-1),\ r_i(n), \frac{1}{i}\}$ *is a probability model for the values of* $r_i(n)$. □

Corollary 2.4. *For any* $n \geq 2$ *and any prime* $p \geq 2$*, the probability* $\mathbb{P}(r_p(n) = 0)$ *that* $r_p(n) = 0$*, and that* p *divides* n*, is* $\frac{1}{p}$*; and the probability* $\mathbb{P}(r_p(n) \neq 0)$ *that* $r_p(n) \neq 0$*, and that* p *does not divide* n*, is* $1 - \frac{1}{p}$. □

We also note the standard definition[24]:

Definition 2. *Two events* e_i *and* e_j *are mutually independent for* $i \neq j$ *if, and only if,* $\mathbb{P}(e_i \cap e_j) = \mathbb{P}(e_i).\mathbb{P}(e_j)$.

[20] The residues $r_i(n)$ can also be graphically displayed variously as shown in the Appendix II in §4..
[21] [HW60], p.49.
[22] See §3., Appendix I; also [Ko56], Chapter I, §1, Axiom III, pg.2.
[23] See §3., Appendix I.
[24] See §3., Appendix I; also [Ko56], Chapter VI, §1, Definition 1, pg.57 and §2, pg.58.

2.C. The prime divisors of any integer n are mutually independent

We then have that:

Lemma 2.5. *If p_i and p_j are two primes where $i \neq j$ then, for any $n \geq 2$, we have:*

$$\mathbb{P}((r_{p_i}(n) = u) \cap (r_{p_j}(n) = v)) = \mathbb{P}(r_{p_i}(n) = u).\mathbb{P}(r_{p_j}(n) = v)$$

where $p_i > u \geq 0$ and $p_j > v \geq 0$.

Proof: The $p_i.p_j$ numbers $v.p_i + u.p_j$, where $p_i > u \geq 0$ and $p_j > v \geq 0$, are all incongruent and form a complete system of residues[25] *mod* $(p_i.p_j)$. Hence:

$$\mathbb{P}((r_{p_i}(n) = u) \cap (r_{p_j}(n) = v)) = \frac{1}{p_i.p_j}$$

By Lemma 2.2:

$$\mathbb{P}(r_{p_i}(n) = u).\mathbb{P}(r_{p_j}(n) = v) = (\tfrac{1}{p_i})(\tfrac{1}{p_j}).$$

The lemma follows. □

If $u = 0$ and $v = 0$ in Lemma 2.5, so that both p_i and p_j are prime divisors of n, we immediately conclude by Definition 2 that:

Corollary 2.6. $\mathbb{P}((r_{p_i}(n) = 0) \cap (r_{p_j}(n) = 0)) = \mathbb{P}(r_{p_i}(n) = 0).\mathbb{P}(r_{p_j}(n) = 0).$ □

We can also express this as:

Corollary 2.7. $\mathbb{P}(p_i|n \ \cap \ p_j|n) = \mathbb{P}(p_i|n).\mathbb{P}(p_j|n).$ □

We thus conclude that:

Theorem 2.8. *The prime divisors of any integer n are mutually independent.* □

2.C.a. Integer Factorising cannot be polynomial-time

We digress briefly from our investigation of prime counting functions to note that Theorem 2.8 immediately yields the actively pursued[26] (although prima facie unconnected) computational complexity consequence that no deterministic algorithm[27] can compute a factor of any randomly given integer n in polynomial time[28]!

We note the standard definition[29]:

Definition 3. *A deterministic algorithm computes a number-theoretical function $f(n)$ in polynomial-time if there exists k such that, for all inputs n, the algorithm computes $f(n)$ in $\leq (log_e\ n)^k + k$ steps.*

[25] [HW60], p.52, Theorem 59.
[26] cf. [Cook].
[27] A deterministic algorithm computes a mathematical function which has a unique value for any input in its domain, and the algorithm is a process that produces this particular value as output.
[28] cf. [Cook], p.1; also [Br00], p.1, fn.1.
[29] cf. [Cook], p.1; also [Br00], p.1, fn.1: "For a polynomial-time algorithm the expected running time should be a polynomial in the length of the input, i.e. $O((logN)^c)$ for some constant c".

It then follows from Theorem 2.8 that:

Corollary 2.9. *Any deterministic algorithm that always computes a prime factor of n cannot be polynomial-time.*

Proof: Any computational process that successfully identifies a prime divisor of n must necessarily appeal to at least one logical operation for identifying such a factor.

Since n is a prime if, and only if, it is not divisible by any prime $p \leq \sqrt{n}$, and n may be the square of a prime, it follows from Theorem 2.8 that we necessarily require at least one logical operation for each prime $p \leq \sqrt{n}$ in order to logically determine whether p is a prime divisor of n.

Since the number of such primes is of the order $O(n/log_e\ n)$, the number of computations required by any deterministic algorithm that always computes a prime factor of n cannot be polynomial-time—i.e. of order $O((log_e\ n)^c)$ for any c—in the length of the input n. The corollary follows. □

2.D. The *non-heuristic* probability $\mathbb{P}(n \in \{p\})$ that n is a prime

Since n is a prime if, and only if, it is not divisible by any prime $p \leq \sqrt{n}$, it follows immediately from Lemma 2.2 and Lemma 2.5 that:

Lemma 2.10. *For any $n \geq 2$, the probability $\mathbb{P}(n \in \{p\})$ of an integer n being a prime p is the probability that $r_{p_i}(n) \neq 0$ for any $1 \leq i \leq k$ if $p_k^2 \leq n < p_{k+1}^2$.* □

By Corollary 2.4 we can express this by the *non-heuristic* prime probability function (graphically illustrated in 1.C., Fig.1)[30]:

Theorem 2.11. $\mathbb{P}(n \in \{p\}) = \prod_{i=1}^{\pi(\sqrt{n})}(1 - \frac{1}{p_i}) \sim \frac{2e^{-\gamma}}{log_e n}$. □

It immediately follows that, for any $m > \pi(\sqrt{n})$:

Corollary 2.12. $\mathbb{P}(n \in \{p\}) > \prod_{i=1}^{m}(1 - \frac{1}{p_i})$. □

2.E. The *non-heuristic* prime counting function $\pi_{_L}(n)$

It now follows from Theorem 2.11 that, since $p_{n+1}^2 - p_n^2 \to \infty$ as $n \to \infty$, by the Law of Large Numbers[31], a *non-heuristic* estimate[32] of the number $\pi(n)$ of primes less than or equal to n is the *non-heuristic* prime counting function (graphically illustrated in §1.C., Fig.2):

Definition 4. $\pi_{_L}(n) = \sum_{j=1}^{n} \prod_{i=1}^{\pi(\sqrt{j})}(1 - \frac{1}{p_i})$.

Corollary 2.13. $\pi(n) \sim \pi_{_L}(n)$. □

[30] We note that $Lt_{n\to\infty} log_e n. \prod_{i=1}^{\pi(\sqrt{n})}(1 - \frac{1}{p_i}) = 2.e^{-\lambda} \approx 1.12292\ldots$ ([Gr95], p.13).
[31] See §3., Appendix I; also [Ko56], Chapter VI, §3, p.61; [**?**], pp.52-57.
[32] i.e. 'expected value': see §3., Apendix III. Compare also [HL23], pp.36-37.

2.F. The interval $(p_n^2,\ p_{n+1}^2)$

It also follows immediately from the definition of $\pi(x)$ as the number of primes less than or equal to x that:

Lemma 2.14. $\prod_{i=1}^{\pi(\sqrt{x})}(1-\frac{1}{p_i}) = \prod_{i=1}^{\pi(\sqrt{x+1})}(1-\frac{1}{p_i})$ *for* $p_n^2 \leq x < p_{n+1}^2$. □

We can also generalise the number-theoretic function of Definition 4 as the real-valued function:

Definition 5. $\pi_{_L}(x) = \pi_{_L}(p_n^2) + (x-p_n^2)\prod_{i=1}^{n}(1-\frac{1}{p_i})$ *for* $p_n^2 \leq x < p_{n+1}^2$. □

We note that the graph of $\pi_{_L}(x)$ in the interval $(p_n^2,\ p_{n+1}^2)$ for $n \geq 1$ is now a straight line with gradient $\prod_{i=1}^{n}(1-\frac{1}{p_i})$, as illustrated in §1.C., Fig.2 where we defined $\pi_{_L}(x)$ equivalently by:

$$\pi_{_L}(x) = \sqcap(x) = (x-p_n^2)\prod_{i=1}^{n}(1-\tfrac{1}{p_i}) + \sum_{j=1}^{n-1}(p_{j+1}^2-p_j^2)\prod_{i=1}^{j}(1-\tfrac{1}{p_i}) + 2$$

2.G. The function $\pi_{_L}(x)/\frac{x}{log_e x}$

We consider next the function $\pi_{_L}(x)/\frac{x}{log_e x}$ in the interval $(p_n^2,\ p_{n+1}^2)$:

$$\pi_{_L}(x)/\tfrac{x}{log_e x} = (\pi_{_L}(p_n^2) + (x-p_n^2)\prod_{i=1}^{n}(1-\tfrac{1}{p_i}))/\tfrac{x}{log_e x}$$

This now yields the derivative $(\pi_{_L}(x).\frac{log_e x}{x})'$ in the interval $(p_n^2,\ p_{n+1}^2)$ as:

$$\pi_{_L}(x).(\tfrac{log_e x}{x})' + (\pi_{_L}(x))'.\tfrac{log_e x}{x}$$
$$(\pi_{_L}(p_n^2) + (x-p_n^2)\prod_{i=1}^{n}(1-\tfrac{1}{p_i})).(\tfrac{log_e x}{x})' + (\pi_{_L}(p_n^2) + (x-p_n^2)\prod_{i=1}^{n}(1-\tfrac{1}{p_i}))'.\tfrac{log_e x}{x}$$
$$(\pi_{_L}(p_n^2) + (x-p_n^2)\prod_{i=1}^{n}(1-\tfrac{1}{p_i})).(\tfrac{1}{x^2} - \tfrac{log_e x}{x^2}) + (\prod_{i=1}^{n}(1-\tfrac{1}{p_i})).\tfrac{log_e x}{x}$$

Since $p_n^2 \leq x < p_{n+1}^2$ and $\pi_L(x) \sim \pi(x)$ by the Law of Large Numbers, by Mertens'[33] and Chebyshev's Theorems we can express the above as:

$$\sim (\pi_{_L}(p_n^2) + \tfrac{e^{-\gamma}(x-p_n^2)}{log_e n}).(\tfrac{1}{x^2} - \tfrac{log_e x}{x^2}) + \tfrac{e^{-\gamma}.log_e x}{x.log_e n}$$
$$\sim (\tfrac{\pi_L(p_n^2)}{x} + \tfrac{e^{-\gamma}}{log_e n}(1-\tfrac{p_n^2}{x})).\tfrac{(1-log_e x)}{x} + \tfrac{e^{-\gamma}.log_e x}{x.log_e n}$$
$$\sim (\tfrac{\pi_L(p_n^2)}{p_n^2}.\tfrac{p_n^2}{x} + \tfrac{e^{-\gamma}}{log_e n}(1-\tfrac{p_n^2}{x})).\tfrac{(1-2.log_e p_n)}{p_n^2} + \tfrac{2.e^{-\gamma}.log_e p_n}{p_n^2.log_e n}$$

Since each term $\to 0$ as $n \to \infty$, we conclude that the function $\pi_{_L}(x)/\frac{x}{log_e x}$ does not oscillate but tends to a limit as $x \to \infty$ since:

Lemma 2.15. $(\pi_{_L}(x)/\frac{x}{log_e x})' \in o(1)$. □

2.H. An elementary probability-based proof of the Prime Number Theorem

The above now yields an elementary probability-based proof that:

Theorem 2.16. $\pi(x) \sim x/log_e x$

Proof: By Lemma 2.15 $(\pi_{_L}(x)/\frac{x}{log_e x})' \in o(1)$; whence the function $\pi_{_L}(x)/\frac{x}{log_e x}$ does not oscillate but tends to a limit as $x \to \infty$.

Since $p_{n+1}^2 - p_n^2 \to \infty$ as $n \to \infty$, and $\pi(x) \sim \pi_L(x)$ by the Law of Large Numbers, the theorem follows from Chebyshev's Theorem that $\pi(x) \asymp x/log_e x$. □

[33] [HW60], Theorem 429, p.351.

2.I. An elementary probability-based proof of Dirichlect's Theorem

We consider next Dirichlect's Theorem, which is the assertion that if a and d are co-prime and $1 \leq a < d$, then the arithmetical progression $a + m.d$, where $m \geq 1$, contains an infinitude of (Dirichlect) primes.

We first note that Lemma 2.5 can be extended to prime powers in general[34]:

Lemma 2.17. *If p_i and p_j are two primes where $i \neq j$ then, for any $n \geq 2,\ \alpha, \beta \geq 1$, we have:*

$$\mathbb{P}((r_{p_i^\alpha}(n) = u) \cap (r_{p_j^\beta}(n) = v)) = \mathbb{P}(r_{p_i^\alpha}(n) = u).\mathbb{P}(r_{p_j^\beta}(n) = v)$$

where $p_i^\alpha > u \geq 0$ and $p_j^\beta > v \geq 0$.

Proof: The $p_i^\alpha.p_j^\beta$ numbers $v.p_i^\alpha + u.p_j^\beta$, where $p_i^\alpha > u \geq 0$ and $p_j^\beta > v \geq 0$, are all incongruent and form a complete system of residues[35] *mod* $(p_i^\alpha.p_j^\beta)$. Hence:

$$\mathbb{P}((r_{p_i^\alpha}(n) = u) \cap (r_{p_j^\beta}(n) = v)) = \frac{1}{p_i^\alpha.p_j^\beta}$$

By Lemma 2.2:

$$\mathbb{P}(r_{p_i^\alpha}(n) = u).\mathbb{P}(r_{p_j^\beta}(n) = v) = (\frac{1}{p_i^\alpha})(\frac{1}{p_j^\beta}).$$

The lemma follows. □

If $u = 0$ and $v = 0$ in Lemma 2.17, so that both p_i and p_j are prime divisors of n, we immediately conclude by Definition 2 that:

Corollary 2.18. $\mathbb{P}((r_{p_i^\alpha}(n) = 0) \cap (r_{p_j^\beta}(n) = 0)) = \mathbb{P}(r_{p_i^\alpha}(n) = 0).\mathbb{P}(r_{p_j\beta}(n) = 0)$. □

We can also express this as:

Corollary 2.19. $\mathbb{P}(p_i^\alpha|n \ \cap \ p_j^\beta|n) = \mathbb{P}(p_i^\alpha|n).\mathbb{P}(p_j^\beta|n)$. □

We thus conclude that:

Theorem 2.20. *For any two primes $p \neq q$ and natural numbers $n, \alpha, \beta \geq 1$, whether or not p^α divides n is independent of whether or not q^β divides n.* □

[34] *Hint*: The following arguments may be easier to follow if we visualise the residues $r_{p_i^\alpha}(n)$ and $r_{p_i^\beta}(n)$ as they would occur in §4., Fig.3 and Fig.4.

[35] [HW60], p.52, Theorem 59.

2.I.a. The probability that n is a prime of the form $a + m.d$

We note next that:

Lemma 2.21. *For any co-prime natural numbers* $1 \leq a < d = q_1^{\alpha_1}.q_2^{\alpha_2} \dots q_k^{\alpha_k}$ *where:*

$q_1 < q_2 < \dots < q_k$ *are primes and* $\alpha_1, \alpha_2 \dots \alpha_k \geq 1$ *are natural numbers;*

the natural number n *is of the form* $a + m.d$ *for some natural number* $m \geq 1$ *if, and only if:*

$$a + r_{q_i^{\alpha_i}}(n) \equiv 0 \ (mod\ q_i^{\alpha_i}) \text{ for all } 1 \leq i \leq k$$

where $0 \leq r_i(n) < i$ *is defined for all* $i > 1$ *by:*

$$n + r_i(n) \equiv 0 \ (mod\ i) \ .$$

Proof: First, if n is of the form $a + m.d$ for some natural number $m \geq 1$, where $1 \leq a < d = q_1^{\alpha_1}.q_2^{\alpha_2} \dots q_k^{\alpha_k}$, then:

$$\begin{array}{rlcll} & n & \equiv & a \ (mod\ d) & \\ and: & n + r_{q_i^{\alpha_i}}(n) & \equiv & 0 \ (mod\ q_i^{\alpha_i}) & for\ all\ 1 \leq i \leq k \\ whence: & a + r_{q_i^{\alpha_i}}(n) & \equiv & 0 \ (mod\ q_i^{\alpha_i}) & for\ all\ 1 \leq i \leq k \end{array}$$

Second:

$$\begin{array}{rlcll} If: & a + r_{q_i^{\alpha_i}}(n) & \equiv & 0 \ (mod\ q_i^{\alpha_i}) & for\ all\ 1 \leq i \leq k \\ and: & n + r_{q_i^{\alpha_i}}(n) & \equiv & 0 \ (mod\ q_i^{\alpha_i}) & for\ all\ 1 \leq i \leq k \\ then: & n - a & \equiv & 0 \ (mod\ q_i^{\alpha_i}) & for\ all\ 1 \leq i \leq k \\ whence: & n & \equiv & a \ (mod\ d) & \end{array}$$

The Lemma follows. □

By Lemma 2.2, it follows that:

Corollary 2.22. *The probability that* $a + r_{q_i^{\alpha_i}}(n) \equiv 0 \ (mod\ q_i^{\alpha_i})$ *for any* $1 \leq i \leq k$ *is* $\frac{1}{q_i^{\alpha_i}}$. □

By Theorem 2.20, it further follows that:

Corollary 2.23. *The joint probability that* $a + r_{q_i^{\alpha_i}}(n) \equiv 0 \ (mod\ q_i^{\alpha_i})$ *for all* $1 \leq i \leq k$ *is* $\prod_{i=1}^{k} \frac{1}{q_i^{\alpha_i}}$. □

We conclude by Lemma 2.21 that:

Corollary 2.24. *The probability that* n *is of the form* $a + m.d$ *for some natural number* $m \geq 1$, *where* $1 \leq a < d = q_1^{\alpha_1}.q_2^{\alpha_2} \dots q_k^{\alpha_k}$ *is* $\prod_{i=1}^{k} \frac{1}{q_i^{\alpha_i}}$. □

It follows that:

Corollary 2.25. *The probability* $\mathbb{P}(n \in \{p\} \cap n \in \{a + m.d\})$ *that* n *is a Dirichlect prime of the form* $a + m.d$ *for some natural number* $m \geq 1$*, where* $1 \leq a < d = q_1^{\alpha_1}.q_2^{\alpha_2} \dots q_k^{\alpha_k}$ *is:*

$$\prod_{i=1}^{k} \frac{1}{q_i^{\alpha_i}} . \prod_{i=1}^{k} (1 - \frac{1}{q_i})^{-1} . \mathbb{P}(n \in \{p\}).$$

Proof: Since a, d are co-prime, we have by Lemma 2.21 that if n is of the form $a + m.d$ for some natural number $m \geq 1$, where $1 \leq a < d = q_1^{\alpha_1}.q_2^{\alpha_2} \dots q_k^{\alpha_k}$, we have that:

$$\begin{array}{rlcll} & n & \equiv & a \ (mod\ q_i) & for\ all\ 1 \leq i \leq k \\ whilst: & n + r_i(n) & \equiv & 0 \ (mod\ i) & for\ all\ 1 \leq i \\ whence: & a + r_{q_i}(n) & \equiv & 0 \ (mod\ q_i) & for\ all\ 1 \leq i \leq k \\ & r_{q_i}(n) & \neq & 0 & for\ all\ 1 \leq i \leq k \\ and: & q_i & \nmid & n & for\ all\ 1 \leq i \leq k \end{array}$$

Hence, if n is of the form $a + m.d$ for some natural number $m \geq 1$, where $1 \leq a < d = q_1^{\alpha_1}.q_2^{\alpha_2} \dots q_k^{\alpha_k}$ and $(a, d) = 1$, the probability that $q_i \nmid n$ for all $1 \leq i \leq k$ is 1.

By Lemma 2.10, Theorem 2.11 and Theorem 2.20, the probability that any $n \geq q_k^2$ is a Dirichlect prime of the form $a + m.d$ is thus:

$$\begin{aligned} & \prod_{i=1}^{k} \frac{1}{q_i^{\alpha_i}} . \prod_{p \neq q_i for 1 \leq i \leq k}^{2 \leq p \leq \sqrt{n}} (1 - \frac{1}{p}) \\ &= \prod_{i=1}^{k} \frac{1}{q_i^{\alpha_i}} . \prod_{i=1}^{k} (1 - \frac{1}{q_i})^{-1} . \prod_{2 \leq p \leq \sqrt{n}} (1 - \frac{1}{p}) \\ &= \prod_{i=1}^{k} \frac{1}{q_i^{\alpha_i}} . \prod_{i=1}^{k} (1 - \frac{1}{q_i})^{-1} . \prod_{j=1}^{\pi(\sqrt{n})} (1 - \frac{1}{p_j}) \\ &= \prod_{i=1}^{k} \frac{1}{q_i^{\alpha_i}} . \prod_{i=1}^{k} (1 - \frac{1}{q_i})^{-1} . \mathbb{P}(n \in \{p\}) \end{aligned}$$

The Corollary follows. □

2.I.b. Dirichlect's Theorem

It further follows from Theorem 2.11 that, since $p_{n+1}^2 - p_n^2 \to \infty$ as $n \to \infty$, by the Law of Large Numbers[36] a *non-heuristic* estimate of the number $\pi_{(a,d)}(n)$ of Dirichlect primes, of the form $a + m.d$ for some natural number $m \geq 1$ and $1 \leq a < d = q_1^{\alpha_1}.q_2^{\alpha_2} \dots q_k^{\alpha_k}$, that are less than or equal to any $n \geq q_k^2$ is the *non-heuristic* Dirichlect prime counting function:

Definition 6. $\pi_D(n) = \sum_{l=1}^{n} (\prod_{i=1}^{k} \frac{1}{q_i^{\alpha_i}} . \prod_{i=1}^{k} (1 - \frac{1}{q_i})^{-1} . \mathbb{P}(l \in \{p\}))$.

We conclude that:

Lemma 2.26. $\pi_{(a,d)}(n) \sim \pi_D(n) \to \infty$ *as* $n \to \infty$.

Proof: If a, d are co-prime and $1 \leq a < d = q_1^{\alpha_1}.q_2^{\alpha_2} \dots q_k^{\alpha_k}$, we have for any $n \geq q_k^2$:

[36] See §3., Appendix I; also [Ko56], Chapter VI, §3, pg. 61.

$$\begin{aligned}
\pi_{_D}(n) &= \sum_{l=1}^{n}(\prod_{i=1}^{k}\tfrac{1}{q_i^{\alpha_i}}.\prod_{i=1}^{k}(1-\tfrac{1}{q_i})^{-1}.\mathbb{P}(l\in\{p\})) \\
&= \prod_{i=1}^{k}\tfrac{1}{q_i^{\alpha_i}}.\prod_{i=1}^{k}(1-\tfrac{1}{q_i})^{-1}.\pi_{_L}(n) \\
&= \prod_{i=1}^{k}\tfrac{1}{q_i^{\alpha_i}}.\prod_{i=1}^{k}(1-\tfrac{1}{q_i})^{-1}.\sum_{l=1}^{n}\prod_{j=1}^{\pi(\sqrt{l})}(1-\tfrac{1}{p_j}) \\
&\geq \prod_{i=1}^{k}\tfrac{1}{q_i^{\alpha_i}}.\prod_{i=1}^{k}(1-\tfrac{1}{q_i})^{-1}.n.\prod_{j=1}^{\pi(\sqrt{n})}(1-\tfrac{1}{p_j})
\end{aligned}$$

The lemma follows since, by Mertens' Theorem, we have that:

$$n.\prod_{j=1}^{\pi(\sqrt{n})}(1-\tfrac{1}{p_j}) \sim \tfrac{2e^{-\gamma}n}{log_e(n)} \to \infty \text{ as } n\to\infty. \qquad \square$$

We conclude by the Law of Large Numbers when applied to the interval, $p_{n+1}^2 - p_n^2 \to \infty$ as $n\to\infty$, that:

Theorem 2.27. *There are an infinity of primes in any arithmetic progression $a+m.d$ where $(a,d)=1$*[37]. $\square$

2.J. An elementary probability-based proof that there are infinitely many twin-primes

We next note that, by Theorem 2.11, we can define the twin-prime counting function $\pi_{_T}(n)$, which *non-heuristically* estimates the number $\pi_{_2}(n)$ of twin primes $(p_i,\ p_{i+1}=p_i+2)$ for $3\leq p_i\leq n$ as:

Definition 7. $\pi_{_T}(n)=\sum_{j=1}^{n}\mathbb{P}(j\in\{p\}\ \cap\ j+2\in\{p\})$

In order to estimate $\pi_{_T}(n)$, we first define:

Definition 8. *An integer n is a $\mathbb{TW}$ integer if, and only if, $r_{p_i}(n)\neq 0$ and $r_{p_i}(n)\neq 2$ for all $1\leq i\leq\pi(\sqrt{n})$.*

Since n is a prime if, and only if, it is not divisible by any prime $p\leq\sqrt{n}$, we then have that:

Lemma 2.28. *If n is a $\mathbb{TW}$ integer, then n is a prime.*

Proof: The lemma follows immediately from Definition 8, Definition 1 and Lemma 2.1. $\square$

Lemma 2.29. *If n is a $\mathbb{TW}$ integer, then $n+2$ is either a prime or $p^2_{\pi(\sqrt{n})+1}$.*

Proof: By Definition 8 and Definition 1:

$$\begin{aligned}
r_{p_i}(n) &\neq 2 \text{ for all } 1\leq i\leq\pi(\sqrt{n}) \\
n+2 &\neq \lambda.i \text{ for all } 2\leq i\leq p_{\pi(\sqrt{n})},\ \lambda\geq 1
\end{aligned}$$

Hence, if $n+2$ is divisible by $p_{\pi(\sqrt{n})+1}$, then $n+2=p^2_{\pi(\sqrt{n})+1}$; else it is a prime. $\square$

Since each residue $r_i(n)$ cycles over the i values $(i-1,i-2,\ldots,0)$, these values are all incongruent and form a complete system of residues *mod* i. It thus follows from Definition 8 and Section 2.B. that the probability of $n\geq 9$ being a $\mathbb{TW}$ integer is:

[37] Compare [HW60], p.13, Theorem 15*.

Lemma 2.30. $\mathbb{P}(n \in \{\mathbb{TW}\}) = \prod_{i=2}^{\pi(\sqrt{n})}(1 - \frac{2}{p_i})$. □

The number $\pi_{\mathbb{TW}}(n)$ of $\mathbb{TW}$ integers ≥ 9 but $\leq n$ is thus:

Lemma 2.31. $\pi_{\mathbb{TW}}(n) = \sum_{j=9}^{n} \prod_{i=2}^{\pi(\sqrt{j})}(1 - \frac{2}{p_i})$. □

Since the number of $\mathbb{TW}$ integers such that $n + 2 = p^2_{\pi(\sqrt{n})+1}$ is not more than $\pi(\sqrt{n})$, it also follows that, for $n \geq 9$:

Lemma 2.32. $\pi_{_T}(n) \geq \sum_{j=9}^{n} \prod_{i=2}^{\pi(\sqrt{j})}(1 - \frac{2}{p_i}) - \pi(\sqrt{n})$. □

We further note that:

Theorem 2.33. $\pi_{_T}(n) \to \infty$ *as* $n \to \infty$.

Proof: We have by Lemma 2.32 that, for $n \geq 9$:

$$\begin{aligned}
\pi_{_T}(n) &\geq (n-9).\prod_{i=2}^{\pi(\sqrt{n})}(1 - \tfrac{2}{p_i}) - \pi(\sqrt{n}) \\
&\geq (n-9).\prod_{i=2}^{\pi(\sqrt{n})}(1 - \tfrac{1}{p_i})(1 - \tfrac{1}{(p_i - 1)}) - \pi(\sqrt{n}) \\
&\geq (n-9).\prod_{i=2}^{\pi(\sqrt{n})}(1 - \tfrac{1}{p_i})(1 - \tfrac{1}{p_{i-1}}) - \pi(\sqrt{n}) \\
&\geq (n-9).\prod_{i=2}^{\pi(\sqrt{n})}(1 - \tfrac{1}{p_{i-1}})^2 - \pi(\sqrt{n}) \\
&\geq (n-9).\prod_{i=1}^{n}(1 - \tfrac{1}{p_i})^2 - \pi(\sqrt{n})
\end{aligned}$$

Now, by Chebyshev's and Mertens' Theorems, we have that:

$$\begin{aligned}
(n-9).\prod_{i=1}^{n}(1 - \tfrac{1}{p_i})^2 - \pi(\sqrt{n}) &\sim (n-9).(\tfrac{e^{-\gamma}}{log_e n})^2 - \pi(\sqrt{n}) \\
&\sim e^{-2\gamma}.\tfrac{n}{log_e^2 n} - \tfrac{9e^{-2\gamma}}{log_e^2 n} - O(\tfrac{\sqrt{n}}{log_e n}) \\
&\to \infty \; as \; n \to \infty
\end{aligned}$$

The theorem follows. □

Since $p^2_{n+1} - p^2_n \to \infty$ as $n \to \infty$, it follows by the Law of Large Numbers that $\pi_{_2}(n) \sim \pi_{_T}(n) \sim \pi_{_{TW}}(n)$. We conclude that there are infinitely many twin primes, and that[38]:

Corollary 2.34. $\pi_{_2}(n) \sim e^{-2\gamma}.\frac{n}{log_e^2 n}$. □

2.K. The Generalised Prime Counting Function: $\sum_{j=1}^{n} \prod_{i=a}^{\pi(\sqrt{j})}(1 - \frac{b}{p_i})$

We note that the argument of Theorem 2.33 in §2.J. is a special case of the limiting behaviour of the Generalised Prime Counting Function $\sum_{j=1}^{n} \prod_{i=a}^{\pi(\sqrt{j})}(1 - \frac{b}{p_i})$, which estimates the number of integers $\leq n$ such that there are b values that cannot occur amongst the residues $r_{p_i}(n)$ for $a \leq i \leq \pi(\sqrt{j})$[39]:

[38] Where $e^{-2\gamma} = 0.3152373316\ldots$; compare [HW60], p.371, §22.20: $\pi_{_2}(n) \sim 2C_2.\frac{n}{log_e^2 n}$, where $C_2 = \prod_{p \geq 3} \frac{p(p-2)}{(p-1)^2} \approx 0.66016181584\ldots$.

[39] Thus $b = 1$ yields an estimate for the number of primes $\leq n$, and $b = 2$ an estimate for the number of TW primes (Definition 8) $\leq n$.

Theorem 2.35. $\sum_{j=1}^{n} \prod_{i=a}^{\pi(\sqrt{j})}(1-\frac{b}{p_i}) \to \infty$ *as* $n \to \infty$ *if* $p_a > b \geq 1$.

Proof: For $p_a > b \geq 1$, we have that:

$$\begin{aligned}
\sum_{j=1}^{n} \prod_{i=a}^{\pi(\sqrt{j})}(1-\tfrac{b}{p_i}) &\geq \sum_{j=p_a^2}^{n} \prod_{i=a}^{\pi(\sqrt{j})}(1-\tfrac{b}{p_i}) \\
&\geq \sum_{j=p_a^2}^{n} \prod_{i=a}^{\pi(\sqrt{n})}(1-\tfrac{b}{p_i}) \\
&\geq (n-p_a^2).\prod_{i=a}^{\pi(\sqrt{n})}(1-\tfrac{b}{p_i}) \\
&\geq (n-p_a^2).\prod_{i=a}^{n}(1-\tfrac{b}{p_i})
\end{aligned}$$

The theorem follows if:

$$log_e(n-p_a^2) + \sum_{i=a}^{n} log_e(1-\tfrac{b}{p_i}) \to \infty$$

(i) We note first the standard result for $|x| < 1$ that:

$$log_e(1-x) = -\sum_{m=1}^{\infty} \tfrac{x^m}{m}$$

For any $p_i > b \geq 1$, we thus have:

$$log_e(1-\tfrac{b}{p_i}) = -\sum_{m=1}^{\infty} \tfrac{(b/p_i)^m}{m} = -\tfrac{b}{p_i} - \sum_{m=2}^{\infty} \tfrac{(b/p_i)^m}{m}$$

Hence:

$$\sum_{i=a}^{n} log_e(1-\tfrac{b}{p_i}) = -\sum_{i=a}^{n}(\tfrac{b}{p_i}) - \sum_{i=a}^{n}(\sum_{m=2}^{\infty} \tfrac{(b/p_i)^m}{m})$$

(ii) We note next that, for all $i \geq a$:

$$c < (1-\tfrac{b}{p_a}) \to c < (1-\tfrac{b}{p_i})$$

It follows for any such c that:

$$\sum_{m=2}^{\infty} \tfrac{(b/p_i)^m}{m} \leq \sum_{m=2}^{\infty}(\tfrac{b}{p_i})^m = \tfrac{(b/p_i)^2}{1-b/p_i} \leq \tfrac{b^2}{c.p_i^2}$$

Since:

$$\sum_{i=1}^{\infty} \tfrac{1}{p_i^2} = O(1)$$

it further follows that:

$$\sum_{i=a}^{n}(\sum_{m=2}^{\infty} \tfrac{(b/p_i)^m}{m}) \leq \sum_{i=a}^{n}(\tfrac{b^2}{c.p_i^2}) = O(1)$$

(iii) From the standard result[40]:

$$\sum_{p \leq x} \frac{1}{p} = log_e log_e x + O(1) + o(1)$$

it then follows that:

$$\begin{aligned} \sum_{i=a}^{n} log_e(1 - \frac{b}{p_i}) &\geq -\sum_{i=a}^{n}(\frac{b}{p_i}) - O(1) \\ &\geq -b.(log_e log_e n + O(1) + o(1)) - O(1) \end{aligned}$$

The theorem follows since:

$$log_e(n - p_a^2) - b.(log_e log_e n + O(1) + o(1)) - O(1) \to \infty$$

and so:

$$log_e(n - p_a^2) + \sum_{i=a}^{n} log_e(1 - \frac{b}{p_i}) \to \infty$$

□

3. Appendix I: Definitions of some terms and concepts of Probability Theory

Probability model[41]: *A probability model* is a mathematical representation of a random phenomenon. It is defined by its sample space, events within the sample space, and probabilities associated with each event.

- *The sample space* S for a probability model is the set of all possible outcomes.
- *An event* A is a subset of the sample space S.
- *A probability* is a numerical value assigned to a given event A.

Distribution Function[42]: Let X be a random variable which denotes the value of the outcome of a certain experiment, and assume that this experiment has only finitely many possible outcomes. Let Ω be the sample space of the experiment (i.e., the set of all possible values of X, or equivalently, the set of all possible outcomes of the experiment). A *distribution function* for X is a real-valued function m whose domain is Ω and which satisfies:

1. $m(\omega) \geq 0$, for all $\omega \in n$, and
2. $\sum_{\omega \in \Omega} m(\omega) = 1$.

For any subset E of Ω, we define the *probability* of E to be the number $P(E)$ given by

$$P(E) = \sum_{\omega \in E} m(\omega)$$

Some notations[43]: Let A and B be two sets. Then the union of A and B is the set

[40] [HW60], p.351, Theorem 427.
[41] cf. http://www.stat.yale.edu/Courses/1997-98/101/probint.htm.
[42] Excerpted from [GS97], Chapter 1, §1.2, p.19.
[43] Excerpted from [GS97], Chapter 1, §1.2, p.21.

$$A \cup B = \{x \mid x \in A \text{ or } x \in B\}$$

The intersection of A and B is the set

$$A \cap B = \{x \mid x \in A \text{ and } x \in B\}$$

The difference of A and B is the set

$$A - B = \{x \mid x \in A \text{ and } x \notin B\}$$

The set A is a subset of B, written $A \subset B$, if every element of A is also an element of B. Finally, the complement of A is the set

$$\overline{A} = \{x \mid x \in \Omega \text{ and } x \notin A\}.$$

Mutual Independence[44]: A set of events $\{A_1,\ A_2,\ \ldots,\ A_n\}$ is said to be *mutually independent* if for any subset $\{A_i,\ A_j,\ \ldots,\ A_m\}$ of these events we have

$$P(A_i \cap A_j \cap \ldots \cap A_m) = P(A_i)P(A_j)\ldots P(A_m),$$

or equivalently, if for any sequence $\overline{A_1},\ \overline{A_2},\ \ldots,\ \overline{A_n}$ with $\overline{A_j} = A_j$ or $\overline{A_j}$,

$$P(\overline{A_i} \cap \overline{A_j} \cap \ldots \cap \overline{A_m}) = P(\overline{A_i})P(\overline{A_j})\ldots P(\overline{A_m}).$$

Expected Value[45]: Let X be a numerically-valued discrete random variable with sample space Ω and distribution function $m(x)$. The *expected value* $E(X)$ is defined by:

$$E(X) = \sum_{x \in \Omega} xm(x),$$

provided this sum converges absolutely. We often refer to the expected value as the mean, and denote $E(X)$ by μ for short. If the above sum does not converge absolutely, then we say that X does not have an expected value.

Law of Large Numbers[46]: Let $X_1,\ X_2,\ \ldots,\ X_n$ be an independent trials process, with finite expected value $\mu = E(X_j)$ and finite variance $\sigma^2 = V(X_j)$. Let $S_n = X_1 + X_2 + \ldots + X_n$. Then for any $\epsilon > 0$,

$$P(|\tfrac{S_n}{n} - \mu| \geq \epsilon) \to 0$$

as $n \to \infty$. Equivalently,

$$P(|\tfrac{S_n}{n} - \mu| < \epsilon) \to 1$$

as $n \to \infty$.

[44] Excerpted from [GS97], Chapter 4, §4.1, Definition 4.2, p.141.
[45] Excerpted from [GS97], Chapter 5, §5.1, p.183.
[46] Excerpted from [GS97], Chapter 8, §8.1, p.307, Theorem 8.2.

4. Appendix II: The residue function $r_i(n)$

We graphically illustrate how the residues $r_i(n)$ occur naturally as values of:

A: The natural-number based residue functions $R_i(n)$;

B: The natural-number based residue sequences $E(n)$;

and as the output of:

C: The natural-number based algorithm $E_{\mathbb{N}}$;

D: The prime-number based algorithm $E_{\mathbb{P}}$;

E: The prime-number based algorithm $E_{\mathbb{Q}}$.

A: The natural-number based residue functions $R_i(n)$

The residues $r_i(n)$ can be defined for all $n \geq 1$ as the values of the natural-number based residue functions $R_i(n)$, defined for all $i \geq 1$ as below in Fig.3. We note that each function $R_i(n)$ cycles through the values $(i-1,\ i-2,\ \ldots,\ 0)$ with period i.

Fig.3: The natural-number based residue functions $R_i(n)$

Function:	$R_1 n$	$R_2 n$	$R_3 n$	$R_4 n$	$R_5 n$	$R_6 n$	$R_7 n$	$R_8 n$	$R_9 n$	$R_{10} n$	$R_{11} n$	$\ldots R_n n$
$n = 1$	0	1	2	3	4	5	6	7	8	9	10	... n-1
$n = 2$	0	0	1	2	3	4	5	6	7	8	9	... n-2
$n = 3$	0	1	0	1	2	3	4	5	6	7	8	... n-3
$n = 4$	0	0	2	0	1	2	3	4	5	6	7	... n-4
$n = 5$	0	1	1	3	0	1	2	3	4	5	6	... n-5
$n = 6$	0	0	0	2	4	0	1	2	3	4	5	... n-6
$n = 7$	0	1	2	1	3	5	0	1	2	3	4	... n-7
$n = 8$	0	0	1	0	2	4	6	0	1	2	3	... n-8
$n = 9$	0	1	0	3	1	3	5	7	0	1	2	... n-9
$n = 10$	0	0	2	2	0	2	4	6	8	0	1	... n-10
$n = 11$	0	1	1	1	4	1	3	5	7	9	0	... n-11
n	$r_1 n$	$r_2 n$	$r_3 n$	$r_4 n$	$r_5 n$	$r_6 n$	$r_7 n$	$r_8 n$	$r_9 n$	$r_{10} n$	$r_{11} n$	$\ldots 0$

Fig.3: The natural-number based residue functions $R_i(n)$

B: The natural-number based residue sequences $E(n)$

The above residues $r_i(n)$ can also be viewed alternatively as values of the associated residue sequences, $E(n) = \{r_i(n) : i \geq 1\}$, defined for all $n \geq 1$, as illustrated below in Fig.4.

We note that:

- The sequences highlighted in red identify a prime[47] p (since $r_i(p) \neq 0$ for $1 < i < p$);
- The 'boundary' residues $r_1(n) = 0$ and $r_n(n) = 0$ are identified in cyan.

[47] Conventionally defined as integers that are not divisible by any smaller integer other than 1.

Fig.4: The natural-number based residue sequences $E(n)$

Function:	R_1n	R_2n	R_3n	R_4n	R_5n	R_6n	R_7n	R_8n	R_9n	$R_{10}n$	$R_{11}n$	$\ldots R_nn$
$E(1)$:	0	1	2	3	4	5	6	7	8	9	10	...n-1
$E(2)$:	0	0	1	2	3	4	5	6	7	8	9	...n-2
$E(3)$:	0	1	0	1	2	3	4	5	6	7	8	...n-3
$E(4)$:	0	0	2	0	1	2	3	4	5	6	7	...n-4
$E(5)$:	0	1	1	3	0	1	2	3	4	5	6	...n-5
$E(6)$:	0	0	0	2	4	0	1	2	3	4	5	...n-6
$E(7)$:	0	1	2	1	3	5	0	1	2	3	4	...n-7
$E(8)$:	0	0	1	0	2	4	6	0	1	2	3	...n-8
$E(9)$:	0	1	0	3	1	3	5	7	0	1	2	...n-9
$E(10)$:	0	0	2	2	0	2	4	6	8	0	1	...n-10
$E(11)$:	0	1	1	1	4	1	3	5	7	9	0	...n-11
...												
$E(n)$:	r_1n	r_2n	r_3n	r_4n	r_5n	r_6n	r_7n	r_8n	r_9n	$r_{10}n$	$r_{11}n$	...0
...												

Fig.4: The natural-number based residue sequences $E(n)$

C: The output of a natural-number based algorithm $E_{\mathbb{N}}$

We give below in Fig.5 the output for $1 \leq n \leq 11$ of a natural-number based algorithm $E_{\mathbb{N}}$ that computes the values $r_i(n)$ of the sequence $E_{\mathbb{N}}(n)$ for only $1 \leq i \leq n$ for any given n.

Fig.5: The output of the natural-number based algorithm $E_{\mathbb{N}}$

Divisors:	1	2	3	4	5	6	7	8	9	10	11	...n...
$E_{\mathbb{N}}(1)$:	0											
$E_{\mathbb{N}}(2)$:	0	0										
$E_{\mathbb{N}}(3)$:	0	1	0									
$E_{\mathbb{N}}(4)$:	0	0	2	0								
$E_{\mathbb{N}}(5)$:	0	1	1	3	0							
$E_{\mathbb{N}}(6)$:	0	0	0	2	4	0						
$E_{\mathbb{N}}(7)$:	0	1	2	1	3	5	0					
$E_{\mathbb{N}}(8)$:	0	0	1	0	2	4	6	0				
$E_{\mathbb{N}}(9)$:	0	1	0	3	1	3	5	7	0			
$E_{\mathbb{N}}(10)$:	0	0	2	2	0	2	4	6	8	0		
$E_{\mathbb{N}}(11)$:	0	1	1	1	4	1	3	5	7	9	0	
...												
$E_{\mathbb{N}}(n)$:	r_1n	r_2n	r_3n	r_4n	r_5n	r_6n	r_7n	r_8n	r_9n	$r_{10}n$	$r_{11}n$	...0
...												

Fig.5: The output of the natural-number based algorithm $E_{\mathbb{N}}$

D: The output of the prime-number based algorithm $E_{\mathbb{P}}$

We give below in Fig.6 the output for $2 \leq n \leq 31$ of a prime-number based algorithm $E_{\mathbb{Q}}$ that computes the values $q_i(n) = r_{p_i}(n)$ of the sequence $E_{\mathbb{P}}(n)$ for only each prime $2 \leq p_i \leq n$ for any given n.

Fig.6: The output of the prime-number based algorithm $E_{\mathbb{P}}$

Prime:	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8	p_9	p_{10}	p_{11}	$\ldots p_n \ldots$
Divisor:	2	3	5	7	11	13	17	19	23	29	31	$\ldots p_n \ldots$
$E_{\mathbb{P}}(2)$:	0											
$E_{\mathbb{P}}(3)$:	1	0										
$E_{\mathbb{P}}(4)$:	0	2										
$E_{\mathbb{P}}(5)$:	1	1	0									
$E_{\mathbb{P}}(6)$:	0	0	4									
$E_{\mathbb{P}}(7)$:	1	2	3	0								
$E_{\mathbb{P}}(8)$:	0	1	2	6								
$E_{\mathbb{P}}(9)$:	1	0	1	5								
$E_{\mathbb{P}}(10)$:	0	2	0	4								
$E_{\mathbb{P}}(11)$:	1	1	4	3	0							
$E_{\mathbb{P}}(12)$:	0	0	3	2	10							
$E_{\mathbb{P}}(13)$:	1	2	2	1	9	0						
$E_{\mathbb{P}}(14)$:	0	1	1	0	8	12						
$E_{\mathbb{P}}(15)$:	1	0	0	6	7	11						
$E_{\mathbb{P}}(16)$:	0	2	4	5	6	10						
$E_{\mathbb{P}}(17)$:	1	1	3	4	5	9	0					
$E_{\mathbb{P}}(18)$:	0	0	2	3	4	8	16					
$E_{\mathbb{P}}(19)$:	1	2	1	2	3	7	15	0				
$E_{\mathbb{P}}(20)$:	0	1	0	1	2	6	14	18				
$E_{\mathbb{P}}(21)$:	1	0	4	0	1	5	13	17				
$E_{\mathbb{P}}(22)$:	0	2	3	6	0	4	12	16				
$E_{\mathbb{P}}(23)$:	1	1	2	5	10	3	11	15	0			
$E_{\mathbb{P}}(24)$:	0	0	1	4	9	2	10	14	22			
$E_{\mathbb{P}}(25)$:	1	2	0	3	8	1	9	13	21			
$E_{\mathbb{P}}(26)$:	0	1	4	2	7	0	8	12	20			
$E_{\mathbb{P}}(27)$:	1	0	3	1	6	12	7	11	19			
$E_{\mathbb{P}}(28)$:	0	2	2	0	5	11	6	10	18			
$E_{\mathbb{P}}(29)$:	1	1	1	6	4	10	5	9	17	0		
$E_{\mathbb{P}}(30)$:	0	0	0	5	3	9	4	8	16	28		
$E_{\mathbb{P}}(31)$:	1	2	4	4	2	8	3	7	15	27	0	
...												
$E_{\mathbb{P}}(n)$:	$q_1 n$	$q_2 n$	$q_3 n$	$q_4 n$	$q_5 n$	$q_6 n$	$q_7 n$	$q_8 n$	$q_9 n$	$q_{10} n$	$q_{11} n$	$\ldots 0$
...												

Fig.6: The output of the prime-number based algorithm $E_{\mathbb{P}}$

E: The output of the prime-number based algorithms $E_{\mathbb{P}}$ and $E_{\mathbb{Q}}$

We give below in Fig.7 the output for $2 \leq n \leq 121$ of the two prime-number based algorithms $E_{\mathbb{P}}$ (whose output $\{q_i(n) = r_{p_i}(n) : 1 \leq i \leq \pi(n)\}$ is shown only partially, partly in cyan) and $E_{\mathbb{Q}}$ (whose

output $q_i(n) = \{r_{p_i}(n) : 1 \leq i \leq \pi(\sqrt{n})\}$ is highlighted in black and red, the latter indicating the generation of a prime sequence and, ipso facto, definition of the corresponding prime[48].

Fig.7: The output of the prime-number based algorithms $E_{\mathbb{P}}$ and $E_{\mathbb{Q}}$

Prime:	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8	p_9	p_{10}	p_{11}	$\ldots p_n \ldots$
Divisor:	2	3	5	7	11	13	17	19	23	29	31	$\ldots p_n \ldots$
Function:	$Q_1 n$	$Q_2 n$	$Q_3 n$	$Q_4 n$	$Q_5 n$	$Q_6 n$	$Q_7 n$	$Q_8 n$	$Q_9 n$	$Q_{10} n$	$Q_{11} n$	$\ldots$
$E_{\mathbb{Q}}(2)$:	0	(Prime by definition)										
$E_{\mathbb{Q}}(3)$:	1	0										
$E_{\mathbb{Q}}(4)$:	0	2										
$E_{\mathbb{Q}}(5)$:	1	1	0									
$E_{\mathbb{Q}}(6)$:	0	0	4									
$E_{\mathbb{Q}}(7)$:	1	2	3	0								
$E_{\mathbb{Q}}(8)$:	0	1	2	6								
$E_{\mathbb{Q}}(9)$:	1	0	1	5								
$E_{\mathbb{Q}}(10)$:	0	2	0	4								
$E_{\mathbb{Q}}(11)$:	1	1	4	3	0							
$E_{\mathbb{Q}}(12)$:	0	0	3	2	10							
$E_{\mathbb{Q}}(13)$:	1	2	2	1	9	0						
$E_{\mathbb{Q}}(14)$:	0	1	1	0	8	12						
$E_{\mathbb{Q}}(15)$:	1	0	0	6	7	11						
$E_{\mathbb{Q}}(16)$:	0	2	4	5	6	10						
$E_{\mathbb{Q}}(17)$:	1	1	3	4	5	9	0					
$E_{\mathbb{Q}}(18)$:	0	0	2	3	4	8	16					
$E_{\mathbb{Q}}(19)$:	1	2	1	2	3	7	15	0				
$E_{\mathbb{Q}}(20)$:	0	1	0	1	2	6	14	18				
$E_{\mathbb{Q}}(21)$:	1	0	4	0	1	5	13	17				
$E_{\mathbb{Q}}(22)$:	0	2	3	6	0	4	12	16				
$E_{\mathbb{Q}}(23)$:	1	1	2	5	10	3	11	15	0			
$E_{\mathbb{Q}}(24)$:	0	0	1	4	9	2	10	14	22			
$E_{\mathbb{Q}}(25)$:	1	2	0	3	8	1	9	13	21			
$E_{\mathbb{Q}}(26)$:	0	1	4	2	7	0	8	12	20			
$E_{\mathbb{Q}}(27)$:	1	0	3	1	6	12	7	11	19			
$E_{\mathbb{Q}}(28)$:	0	2	2	0	5	11	6	10	18			
$E_{\mathbb{Q}}(29)$:	1	1	1	6	4	10	5	9	17	0		
$E_{\mathbb{Q}}(30)$:	0	0	0	5	3	9	4	8	16	28		
$E_{\mathbb{Q}}(31)$:	1	2	4	4	2	8	3	7	15	27	0	
$E_{\mathbb{Q}}(32)$:	0	1	3	3	1	7	2	6	14	26	30	
$E_{\mathbb{Q}}(33)$:	1	0	2	2	0	6	1	5	13	25	29	
$E_{\mathbb{Q}}(34)$:	0	2	1	1	10	5	0	4	12	24	28	
$E_{\mathbb{Q}}(35)$:	1	1	0	0	9	4	16	3	11	23	27	
$E_{\mathbb{Q}}(36)$:	0	0	4	6	8	3	15	2	10	22	26	
$E_{\mathbb{Q}}(37)$:	1	2	3	5	7	2	14	1	9	21	25	
$E_{\mathbb{Q}}(38)$:	0	1	2	4	6	1	13	0	8	20	24	
$E_{\mathbb{Q}}(39)$:	1	0	1	3	5	0	12	18	7	19	23	

[48] For informal reference and perspective, formal definitions of both the prime-number based algorithms $E_{\mathbb{P}}$ and $E_{\mathbb{Q}}$ are given in this work in progress *Factorising all $m \leq n$ is of order $\Theta(\sum_{i=2}^{n} \pi(\sqrt{i}))$.*

$E_{\mathbb{Q}}(40)$:	0	2	0	2	4	12	11	17	6	18	22
$E_{\mathbb{Q}}(41)$:	1	1	4	1	3	11	10	16	5	17	21
$E_{\mathbb{Q}}(42)$:	0	0	3	0	2	10	9	15	4	16	20
$E_{\mathbb{Q}}(43)$:	1	2	2	6	1	9	8	14	3	15	19
$E_{\mathbb{Q}}(44)$:	0	1	1	5	0	8	7	13	2	14	18
$E_{\mathbb{Q}}(45)$:	1	0	0	4	10	7	6	12	1	13	17
$E_{\mathbb{Q}}(46)$:	0	2	4	3	9	6	5	11	0	12	16
$E_{\mathbb{Q}}(47)$:	1	1	3	2	8	5	4	10	22	11	15
$E_{\mathbb{Q}}(48)$:	0	0	2	1	7	4	3	9	21	10	14
$E_{\mathbb{Q}}(49)$:	1	2	1	0	6	3	2	8	20	9	13
$E_{\mathbb{Q}}(50)$:	0	1	0	6	5	2	1	7	19	8	12
$E_{\mathbb{Q}}(51)$:	1	0	4	5	4	1	0	6	18	7	11
$E_{\mathbb{Q}}(52)$:	0	2	3	4	3	0	16	5	17	6	10
$E_{\mathbb{Q}}(53)$:	1	1	2	3	2	12	15	4	16	5	9
$E_{\mathbb{Q}}(54)$:	0	0	1	2	1	11	14	3	15	4	8
$E_{\mathbb{Q}}(55)$:	1	2	0	1	0	10	13	2	14	3	7
$E_{\mathbb{Q}}(56)$:	0	1	4	0	10	9	12	1	13	2	6
$E_{\mathbb{Q}}(57)$:	1	0	3	6	9	8	11	0	12	1	5
$E_{\mathbb{Q}}(58)$:	0	2	2	5	8	7	10	18	11	0	4
$E_{\mathbb{Q}}(59)$:	1	1	1	4	7	6	9	17	10	28	3
$E_{\mathbb{Q}}(60)$:	0	0	0	3	6	5	8	16	9	27	2
$E_{\mathbb{Q}}(61)$:	1	2	4	2	5	4	7	15	8	26	1
$E_{\mathbb{Q}}(62)$:	0	1	3	1	4	3	6	14	7	25	0
$E_{\mathbb{Q}}(63)$:	1	0	2	0	3	2	5	13	6	24	30
$E_{\mathbb{Q}}(64)$:	0	2	1	6	2	1	4	12	5	23	29
$E_{\mathbb{Q}}(65)$:	1	1	0	5	1	0	3	11	4	22	28
$E_{\mathbb{Q}}(66)$:	0	0	4	4	0	12	2	10	3	21	27
$E_{\mathbb{Q}}(67)$:	1	2	3	3	10	11	1	9	2	20	26
$E_{\mathbb{Q}}(68)$:	0	1	2	2	9	10	0	8	1	19	25
$E_{\mathbb{Q}}(69)$:	1	0	1	1	8	9	16	7	0	18	24
$E_{\mathbb{Q}}(70)$:	0	2	0	0	7	8	15	6	22	17	23
$E_{\mathbb{Q}}(71)$:	1	1	4	6	6	7	14	5	21	16	22
$E_{\mathbb{Q}}(72)$:	0	0	3	5	5	6	13	4	20	15	21
$E_{\mathbb{Q}}(73)$:	1	2	2	4	4	5	12	3	19	14	20
$E_{\mathbb{Q}}(74)$:	0	1	1	3	3	4	11	2	18	13	19
$E_{\mathbb{Q}}(75)$:	1	0	0	2	2	3	10	1	17	12	18
$E_{\mathbb{Q}}(76)$:	0	2	4	1	1	2	9	0	16	11	17
$E_{\mathbb{Q}}(77)$:	1	1	3	0	0	1	8	18	15	10	16
$E_{\mathbb{Q}}(78)$:	0	0	2	6	10	0	7	17	14	9	15
$E_{\mathbb{Q}}(79)$:	1	2	1	5	9	12	6	16	13	8	14
$E_{\mathbb{Q}}(80)$:	0	1	0	4	8	11	5	15	12	7	13
$E_{\mathbb{Q}}(81)$:	1	0	4	3	7	10	4	14	11	6	12
$E_{\mathbb{Q}}(82)$:	0	2	3	2	6	9	3	13	10	5	11
$E_{\mathbb{Q}}(83)$:	1	1	2	1	5	8	2	12	9	4	10
$E_{\mathbb{Q}}(84)$:	0	0	1	0	4	7	1	11	8	3	9
$E_{\mathbb{Q}}(85)$:	1	2	0	6	3	6	0	10	7	2	8
$E_{\mathbb{Q}}(86)$:	0	1	4	5	2	5	16	9	6	1	7
$E_{\mathbb{Q}}(87)$:	1	0	3	4	1	4	15	8	5	0	6
$E_{\mathbb{Q}}(88)$:	0	2	2	3	0	3	14	7	4	28	5
$E_{\mathbb{Q}}(89)$:	1	1	1	2	10	2	13	6	3	27	4

$E_{\mathbb{Q}}(90)$:	0	0	0	1	9	1	12	5	2	26	3
$E_{\mathbb{Q}}(91)$:	1	2	4	0	8	0	11	4	1	25	2
$E_{\mathbb{Q}}(92)$:	0	1	3	6	7	12	10	3	0	24	1
$E_{\mathbb{Q}}(93)$:	1	0	2	5	6	11	9	2	22	23	0
$E_{\mathbb{Q}}(94)$:	0	2	1	4	5	10	8	1	21	22	30
$E_{\mathbb{Q}}(95)$:	1	1	0	3	4	9	7	0	20	21	29
$E_{\mathbb{Q}}(96)$:	0	0	4	2	3	8	6	18	19	20	28
$E_{\mathbb{Q}}(97)$:	1	2	3	1	2	7	5	17	18	19	27
$E_{\mathbb{Q}}(98)$:	0	1	2	0	1	6	4	16	17	18	26
$E_{\mathbb{Q}}(99)$:	1	0	1	6	0	5	3	15	16	17	25
$E_{\mathbb{Q}}(100)$:	0	2	0	5	10	4	2	14	15	16	24
$E_{\mathbb{Q}}(101)$:	1	1	4	4	9	3	1	13	14	15	23
$E_{\mathbb{Q}}(102)$:	0	0	3	3	8	2	0	12	13	14	22
$E_{\mathbb{Q}}(103)$:	1	2	2	2	7	1	16	11	12	13	21
$E_{\mathbb{Q}}(104)$:	0	1	1	1	6	0	15	10	11	12	20
$E_{\mathbb{Q}}(105)$:	1	0	0	0	5	12	14	9	10	11	19
$E_{\mathbb{Q}}(106)$:	0	2	4	6	4	11	13	8	9	10	18
$E_{\mathbb{Q}}(107)$:	1	1	3	5	3	10	12	7	8	9	17
$E_{\mathbb{Q}}(108)$:	0	0	2	4	2	9	11	6	7	8	16
$E_{\mathbb{Q}}(109)$:	1	2	1	3	1	8	10	5	6	7	15
$E_{\mathbb{Q}}(110)$:	0	1	0	2	0	7	9	4	5	6	14
$E_{\mathbb{Q}}(111)$:	1	0	4	1	10	6	8	3	4	5	13
$E_{\mathbb{Q}}(112)$:	0	2	3	0	9	5	7	2	3	4	12
$E_{\mathbb{Q}}(113)$:	1	1	2	6	8	4	6	1	2	3	11
$E_{\mathbb{Q}}(114)$:	0	0	1	5	7	3	5	0	1	2	10
$E_{\mathbb{Q}}(115)$:	1	2	0	4	6	2	4	18	0	1	9
$E_{\mathbb{Q}}(116)$:	0	1	4	3	5	1	3	17	22	0	8
$E_{\mathbb{Q}}(117)$:	1	0	3	2	4	0	2	16	21	28	7
$E_{\mathbb{Q}}(118)$:	0	2	2	1	3	12	1	15	20	27	6
$E_{\mathbb{Q}}(119)$:	1	1	1	0	2	11	0	14	19	26	5
$E_{\mathbb{Q}}(120)$:	0	0	0	6	1	10	16	13	18	25	4
$E_{\mathbb{Q}}(121)$:	1	2	4	5	0	9	15	12	17	24	3
...											
$E_{\mathbb{Q}}(n)$:	$q_1 n$	$q_2 n$	$q_3 n$	$q_4 n$	$q_5 n$	$q_6 n$	$q_7 n$	$q_8 n$	$q_9 n$	$q_{10} n$	$q_{11} n$	...
...												

Prime:	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8	p_9	p_{10}	p_{11}	$\ldots p_n \ldots$
Divisor:	2	3	5	7	11	13	17	19	23	29	31	$\ldots p_n \ldots$

Fig.7: The output of the prime-number based algorithms $E_{\mathbb{P}}$ and $E_{\mathbb{Q}}$

References

[Br00] Richard P. Brent. 2000. *Recent Progress and Prospects for Integer Factorisation Algorithms.* In *Computing and Combinatorics*, Lecture Notes in Computer Science, Volume 1858, 2000, pp.3-22, Springer, New York/Heidelberg.

[Cook] Stephen Cook. 2000. *The P versus NP Problem*. Official description provided for the Clay Mathematical Institute, Cambridge, Massachusetts.

[DiI52] Leonard Eugene Dickson. 1952. *History of the Theory of Numbers: Volume I.* Chelsea Publishing Company, New York, N. Y.

[Dir37] Peter Gustav Lejeune Dirichlet. 1837. *There are infinitely many prime numbers in all arithmetic progressions with first term and difference coprime.* Originally read to The Royal Prussian Academy of Sciences on the 27th of July,

1837; published in *Abhandlungen der Königlichen Preußischen Akademie der Wissenschaften zu Berlin*, 1837, 4581. *Citation source*: English translation and arXive on 24/11/2014 by Ralf Stephan at http://arXiv:0808.1408v2.

[Gr95] Andrew Granville. 1995. *Harald Cramér and the distribution of prime numbers*. Scandinavian Actuarial Journal, Volume 1995, Issue 1, pp.12-28. DOI:10.1080/03461238.1995.10413946.

[GS97] Charles M. Grinstead and J. Laurie Snell. 2003. *Introduction to Probability*, *The CHANCE Project* Version dated 4 July 2006 of the Second Revised Edition, 1997, American Mathematical Society, Rhode Island, USA.

[HL23] G.H Hardy and J.E. Littlewood. 1923. *Some problems of 'partitio numerorum:' III: On the expression of a number as a sum of primes*, Acta Mathematica, December 1923, Volume 44, pp.1-70.

[HW60] G. H. Hardy and E. M. Wright. 1960. *An Introduction to the Theory of Numbers*. 4th edition. Clarendon Press, Oxford.

[Ka59] Mark Kac. 1959. *Statistical Independence in Probability, Analysis and Number Theory*. 1959. *The Carus Mathematical Monographs: Number Twelve* The Mathematical Association of America, Second Impression, 1964.

[Ko56] A. N. Kolmogorov. 1933. *Foundations of the Theory of Probability*. Second English Edition. Translation edited by Nathan Morrison. 1956. Chelsea Publishing Company, New Yourk (*sic*).

[Ri74] Ian Richards. 1974. *On The Incompatibility Of Two Conjectures Concerning Primes; A Discussion Of The Use Of Computers In Attacking A Theoretical Problem*. Bulletin Of The American Mathematical Society, Volume 80, Number 3, May 1974.

[Se49] Atle Selberg. 1949. *An Elementary Proof of Dirichlet's Theorem About Primes in an Arithmetic Progression*. Annals of Mathematics, Second Series, Vol. 50, No. 2 (Apr., 1949), pp. 297-304.

[St02] Jörn Steuding. 2002. *Probabilistic Number Theory*. The Pennsylvania State University CiteSeerX Archives, doi=10.1.1.118.4755.

[An14a] Bhupinder Singh Anand. 2014. *A probability-based proof that any deterministic algorithm which always computes a prime factor of n cannot be polynomial-time*. Submitted on 01/01/2015 to the *Calcutta Statistical Association Bulletin*, Kolkata, India.

[An14b] Bhupinder Singh Anand. 2014. *Defining prime probability analytically: A probability-based approach to estimating the prime and twin-prime counting functions $\pi(n)$ and $\pi_2(n)$ analytically*. Submitted on 12/12/2014 to the *Calcutta Statistical Association Bulletin*, Kolkata, India.

Bhupinder Singh Anand
#1003 B Wing, Lady Ratan Tower
Dainik Shivner Marg
Gandhinagar, Worli
Mumbai - 400 018
Maharashtra, India.
e-mail: bhup.anand@gmail.com