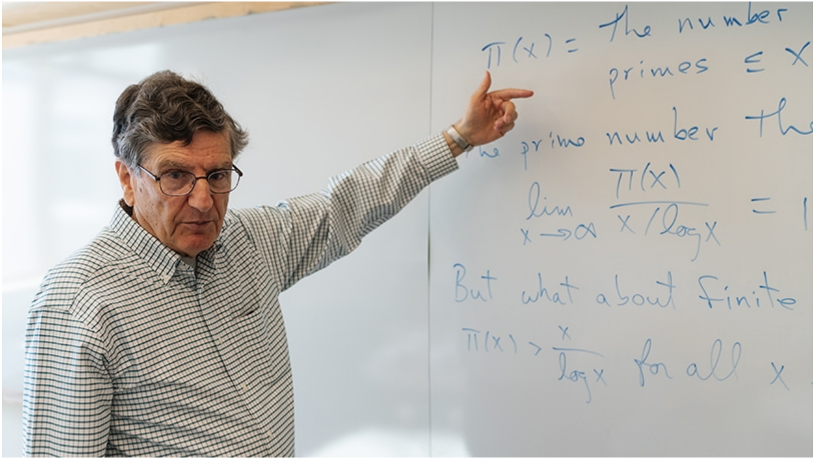
Counting shifted-prime divisors

Steve Fan (UGA)

Inspired by joint work with Carl Pomerance (Dartmouth College)

May 17, 2025



Carl Pomerance

Proof of the Sheldon Conjecture

Carl Pomerance and Chris Spicer

Abstract. In [**3**], the authors introduce the concept of a Sheldon prime, based on a conversation between several characters in the CBS television situation comedy *The Big Bang Theory*. The authors of [**3**] leave open the question of whether 73 is the unique Sheldon prime. This paper answers this question in the affirmative.

1. INTRODUCTION. A Sheldon prime was first defined in [**3**] as an homage to Sheldon Cooper, a fictional theoretical physicist, see Figure 1, on the television show *The Big Bang Theory*, who claimed 73 is the best number because it has some seemingly unusual properties. First note that not only is 73 a prime number, its index in the sequence of primes is the product of its digits, namely 21: it is the 21st prime. In addition, reversing the digits of 73, we obtain the prime 37, which is the 12th prime, and 12 is the reverse of 21.

We give a more formal definition. For a positive integer n, let p_n denote the nth prime number. We say p_n has the *product property* if the product of its base-10 digits is precisely n. For any positive integer x, we define $\operatorname{rev}(x)$ to be the integer whose sequence of base-10 digits is the reverse of the digits of x. For example, $\operatorname{rev}(1234) = 4321$ and $\operatorname{rev}(310) = 13$. We say p_n satisfies the *mirror property* if $\operatorname{rev}(p_n) = p_{\operatorname{rev}(n)}$.

Definition. The prime p_n is a Sheldon prime if it satisfies both the product property and the mirror property.

In [**3**], the "Sheldon Conjecture" was posed that 73 is the only Sheldon prime. In Section 5 we prove the following result.

Theorem 1. *The Sheldon conjecture holds: 73 is the unique Sheldon prime.*

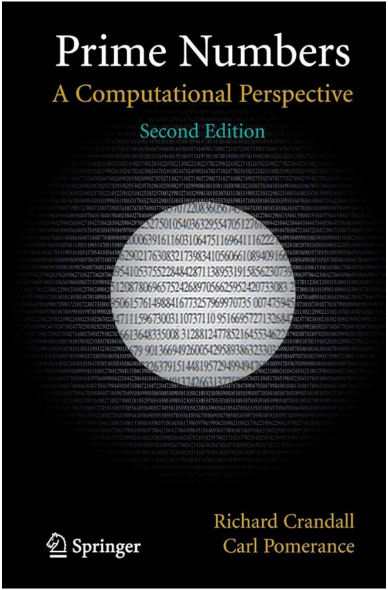
2. THE PRIME NUMBER THEOREM AND SHELDON PRIMES. Let $\pi(x)$ denote the number of prime numbers in the interval $[2, x]$. Looking at tables of primes it appears that they tend to thin out, becoming rarer as one looks at larger numbers. This can be expressed rigorously by the claim that $\lim_{x\to\infty} \pi(x)/x = 0$. In fact, more is true: we know the rate at which the ratio $\pi(x)/x$ tends to 0. This is the prime number theorem:

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1,$$

where "log" is the natural logarithm function. This theorem was first proved in 1896 independently by Hadamard and de la Vallée Poussin, following a general plan laid out by Riemann about 40 years earlier (the same paper where he first enunciated the now famous Riemann hypothesis).

We actually know that $\pi(x)$ is slightly larger than $x/\log x$ for large values of x; in fact there is a secondary term $x/(\log x)^2$, a positive tertiary term, and so on. The phrase "large values of x" can be made numerically explicit: A result of Rosser and Schoenfeld [**7**, (3.5)] is that

$$\pi(x) > \frac{x}{\log x} \text{ for all } x \geq 17. \tag{1}$$



Shifted primes

A *shifted prime* is an integer of the form $p - a$, where p is prime and $a \in \mathbb{Z} \setminus \{0\}$.

We say that $p - a \neq 0$ is a *shifted-prime divisor* of $n \in \mathbb{N}$ if $(p - a) \mid n$.

For each $n \in \mathbb{N}$, denote by $\omega_a^*(n)$ the number of shifted-prime divisors $p - a$ of n:

$$\omega_a^*(n) := \#\{p > a \text{ prime} \colon (p - a) \mid n\}.$$

We will focus mainly on $\omega^*(n) := \omega_1^*(n)$ and visit briefly the general case near the end of the talk.

Example

Shifted-prime divisors $p - 1$ of 24: 1, 2, 4, 6, 12. So $\omega^*(24) = 5$.

The set $\mathbb{P}_a$

The sets $\mathbb{N}$ and $\mathbb{P}_a = \{p - a \colon p > a\}$ are structurally similar in many ways.

- Equidistribution in arithmetic progressions:

$$\frac{1}{x} \cdot \#\{n \in \mathbb{N} \cap [1, x] \colon n \equiv b \pmod{k}\} \sim \frac{1}{k},$$
$$\frac{1}{\pi(x)} \cdot \#\{n \in \mathbb{P}_a \cap [1, x] \colon n \equiv c \pmod{k}\} \sim \frac{1}{\varphi(k)},$$

as $x \to \infty$, where $k \in \mathbb{N}$, $b \in \mathbb{Z}$, and $c \in \mathbb{Z}$ with $\gcd(a + c, k) = 1$.

The set $\mathbb{P}_a$

The sets $\mathbb{N}$ and $\mathbb{P}_a = \{p - a : p > a\}$ are structurally similar in many ways.

- Equidistribution in arithmetic progressions:

$$\frac{1}{x} \cdot \#\{n \in \mathbb{N} \cap [1, x] : n \equiv b \pmod{k}\} \sim \frac{1}{k},$$
$$\frac{1}{\pi(x)} \cdot \#\{n \in \mathbb{P}_a \cap [1, x] : n \equiv c \pmod{k}\} \sim \frac{1}{\varphi(k)},$$

  as $x \to \infty$, where $k \in \mathbb{N}$, $b \in \mathbb{Z}$, and $c \in \mathbb{Z}$ with $\gcd(a + c, k) = 1$.

- Typical number of prime factors: Let $S = \mathbb{N}$ or $\mathbb{P}_a$, and $S_x = S \cap [1, x]$.

  Most numbers n in S have about $\log\log n$ prime factors.

$$\lim_{x \to \infty} \frac{1}{\#S_x} \cdot \#\left\{n \in S_x : \frac{\omega(n) - \log\log n}{\sqrt{\log\log n}} \le T\right\} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{T} e^{-t^2/2}\, dt.$$

  $S = \mathbb{N}$ due to Erdős and Kac (1940) and $S = \mathbb{P}_a$ due to Halberstam (1955).

The set $\mathbb{P}_a$

- Twin primes: Are there infinitely many shifted primes $p+2$ that are prime?

  The recent breakthroughs made by Zhang, Maynard and Polymath, building on early works of Goldston, Pintz and Yıldırım, shows that there exists an even integer $2 \leq a \leq 246$ such that there are infinitely many shifted primes $p+a$ that are prime.

The set $\mathbb{P}_a$

- Twin primes: Are there infinitely many shifted primes $p+2$ that are prime?

  The recent breakthroughs made by Zhang, Maynard and Polymath, building on early works of Goldston, Pintz and Yıldırım, shows that there exists an even integer $2 \leq a \leq 246$ such that there are infinitely many shifted primes $p+a$ that are prime.

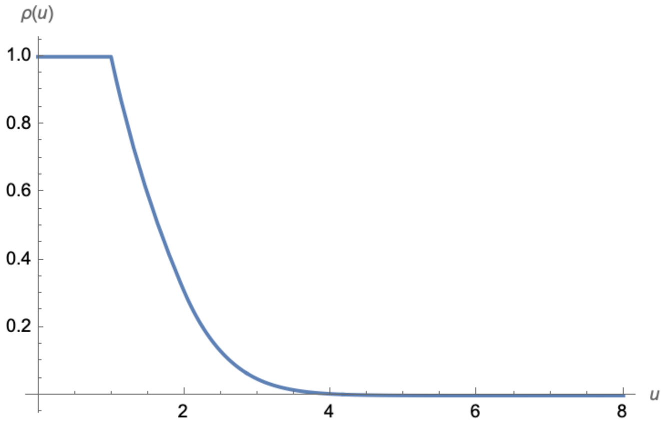
- A conjecture of Pomerance on smooth shifted primes (1980):

$$\frac{1}{\pi(x)} \cdot \# \left\{p \leq x \colon P^+(p-1) \leq y\right\} \sim \frac{1}{x} \cdot \# \left\{n \leq x \colon P^+(n) \leq y\right\}$$

  for $x \geq y$ as $y \to \infty$, where $P^+(m)$ is the largest prime factor of m.

Density of smooth numbers

Figure 1: The Dickman–de Bruijn function $\rho(u)$ on $[1, 8]$



$$\frac{1}{x} \cdot \#\{n \leq x \colon P^+(n) \leq x^{1/u}\} \approx \rho(u).$$

The function ω^*

The function

$$\omega^*(n) := \sum_{(p-1)|n} 1$$

was first introduced by Prachar (1955). It has played important roles in

- the 1983 development of the first unconditional deterministic primality test, running in nearly polynomial time, by Adleman, Pomerance and Rumely,
- the study of Carmichael numbers:

  A Carmichael number n is a composite number satisfying $b^n \equiv b \pmod{n}$ for all $b \in \mathbb{Z}$. Korselt showed in 1899 that $n \in \mathbb{N}$ is a Carmichael number if and only if n is square-free, and $p \mid n \Rightarrow p - 1 \mid n - 1$. Alford, Granville and Pomerance (1994) proved that for sufficiently large x, the interval $[1, x]$ contains at least $x^{2/7}$ Carmichael numbers. The exponent "$2/7$" has been improved to 0.332 by Harman (2005) and to 0.3389 by Lichtman (2022).

The maximal order of ω^*

The minimal order of ω^* is trivially 1: $\omega^*(n) = 1$ for odd $n \in \mathbb{N}$.

For the maximal orders, we have

$$\limsup_{x\to\infty} \frac{\omega(n)}{\log n/\log\log n} = 1,$$
$$\limsup_{x\to\infty} \frac{\log\tau(n)}{\log n/\log\log n} = \log 2. \quad \text{(Wigert, 1907)}$$

Prachar (1955) showed that for infinitely many n,

$$\omega^*(n) > \exp\left(c_1 \frac{\log n}{(\log\log n)^2}\right) \quad \text{(unconditionally)},$$
$$\omega^*(n) > \exp\left(\left(\frac{1}{2}\log 2 - \epsilon\right)\frac{\log n}{\log\log n}\right) \quad \text{(under GRH)},$$

where $c_1 > 0$ is some absolute constant, and $\epsilon > 0$ is fixed but otherwise arbitrary.

The maximal order of ω^*

Adleman, Pomerance and Rumely (1983) removed one $\log\log n$ factor from Prachar's unconditional bound, obtaining

$$\omega^*(n) > \exp\left(c_2 \frac{\log n}{\log\log n}\right)$$

for infinitely many n, where $c_2 > 0$ is some absolute computable constant.

They also conjectured that one can take $c_2 = \log 2 - \epsilon$ for any $\epsilon > 0$. This conjecture, if true, would imply that the minimal order of the Carmichael function $\lambda(n) := \mathrm{Exp}(\mathbb{Z}/n\mathbb{Z})^\times$ is

$$\exp\left(\frac{1}{\log 2}(\log\log n)\log\log\log n\right),$$

as indicated in Erdős, Pomerance, and Schmutz (1991).

The maximal order of ω^*

Recently, Pollack and I examined Prachar's proof of his GRH-conditional estimate and observed the following:

1. The Adleman–Pomerance–Rumely conjecture holds if given any $\epsilon \in (0,1)$,

$$\pi(x;q,1) := \#\{p \le x : p \equiv 1 \pmod q\} \gg_\epsilon \frac{\pi(x)}{\varphi(q)}$$

for $q \mid \prod_{p \le (1-\epsilon)\log x} p$ possibly with extremely rare exceptions.

The maximal order of ω^*

Recently, Pollack and I examined Prachar's proof of his GRH-conditional estimate and observed the following:

1. The Adleman–Pomerance–Rumely conjecture holds if given any $\epsilon \in (0,1)$,
$$\pi(x;q,1) := \#\{p \le x : p \equiv 1 \pmod q\} \gg_\epsilon \frac{\pi(x)}{\varphi(q)}$$
for $q \mid \prod_{p \le (1-\epsilon)\log x} p$ possibly with extremely rare exceptions.
2. The Adleman–Pomerance–Rumely conjecture also follows from Pomerance's conjecture that
$$\frac{1}{\pi(x)} \cdot \#\left\{p \le x : P^+(p-1) \le y\right\} \sim \frac{1}{x} \cdot \#\left\{n \le x : P^+(n) \le y\right\}$$
for $x \ge y$ as $y \to \infty$. It is directly related to lower bounding
$$\sum_{p \le x} \prod_{\substack{q \le (1-\epsilon)\log x \\ q \mid (p-1)}} q.$$

The maximal order of ω^*

3. By modifying Prachar's argument, we found that for infinitely many n,

$$\omega^*(n) > \exp\left(0.6269 \ln 2 \cdot \frac{\log n}{\log\log n}\right) \quad \text{(unconditionally)},$$
$$\omega^*(n) > \exp\left(0.6823 \ln 2 \cdot \frac{\log n}{\log\log n}\right) \quad \text{(under GRH)}.$$

The first inequality is derived from a result on $\pi(x; q, a)$ in Alford, Granville and Pomerance (1994).

The densities $\delta_k(\omega^*)$

For any arithmetic function f, we denote by $\delta_k(f)$ the *natural density* of the level set $\{n \in \mathbb{N} \colon f(n) = k\}$ for each $k \in \mathbb{N}$, namely,

$$\delta_k(f) := \lim_{x \to \infty} \frac{\#\{n \le x \colon f(n) = k\}}{x},$$

provided that this limit exists.

The densities $\delta_k(\omega^*)$

For any arithmetic function f, we denote by $\delta_k(f)$ the *natural density* of the level set $\{n \in \mathbb{N} \colon f(n) = k\}$ for each $k \in \mathbb{N}$, namely,

$$\delta_k(f) := \lim_{x \to \infty} \frac{\#\{n \le x \colon f(n) = k\}}{x},$$

provided that this limit exists. Landau (1900) showed that for every fixed $k \in \mathbb{N}$,

$$\#\{n \le x \colon \omega(n) = k\} \sim \frac{x(\log\log x)^{k-1}}{(k-1)!\log x}$$

as $x \to \infty$. So $\delta_k(\omega) = 0$. Since $\tau(n) \ge 2^{\omega(n)}$, we also have $\delta_k(\tau) = 0$ for every $k \in \mathbb{N}$.

What about $\delta_k(\omega^*)$?

The densities $\delta_k(\omega^*)$

Theorem 1 (F.–Pomerance, 2024)

For every $k \in \mathbb{N}$, the k-level set $\mathcal{L}_k := \{n \in \mathbb{N} \colon \omega^*(n) = k\}$ admits a positive natural density δ_k. Moreover, we have $\sum_{k\geq 1} \delta_k = 1$.

The key step in establishing Theorem 1 is to verify $\mathcal{L}_k \neq \emptyset$. The proof makes use of Chen's theorem:

$$\mathcal{P}_2(x) := \{2 < p \leq x \colon \Omega((p-1)/2) \leq 2 \text{ and } P^-((p-1)/2) > x^{3/11}\} \gg \frac{x}{(\log x)^2}.$$

Fixing $n \in 2\mathbb{N}$, we wish to find some large $p \in \mathcal{P}_2(x)$ such that

$$\omega^*(n(p-1)/2) = \omega^*(n) + 1.$$

If $p \in \mathcal{P}_2(x)$ fails this property, then there are $a \mid n$ and $b \mid (p-1)/2$ with $a, b > 1$ such that $ab + 1$ a prime $\neq p$.

1. $b = (p-1)/2$ with $ab + 1$ is prime with $a > 2$
2. $p - 1 = 2qb$ with $ab + 1$ prime, where $q, r \in (x^{3/11}, x^{8/11})$.

The densities $\delta_k(\omega^*)$

1. $b = (p-1)/2$ and $ab+1$ is prime with $a > 2$

   This means that (i) $P^-(b) > x^{3/11}$, and (ii) $2b+1$ and $ab+1$ are both prime. Given a, the count for p is $O(x/(\log x)^3)$.

The densities $\delta_k(\omega^*)$

1. $b = (p-1)/2$ and $ab+1$ is prime with $a > 2$

   This means that (i) $P^-(b) > x^{3/11}$, and (ii) $2b+1$ and $ab+1$ are both prime. Given a, the count for p is $O(x/(\log x)^3)$.

2. $p - 1 = 2qb$ with $aq+1$ prime, where $q, r \in (x^{3/11}, x^{8/11})$.

   For any $q \in (x^{3/11}, x^{8/11})$, the number of primes $b < x/2q$ such that both $ab+1$ and $2qb+1$ are prime is

$$\ll \frac{x}{q(\log x)^3} \prod_{r|(2q-a)} \left(1 - \frac{1}{r}\right)^{-1} \ll \frac{\log\log q}{q} \cdot \frac{x}{(\log x)^3}.$$

   Summing this bound on $q \in (x^{3/11}, x^{8/11})$ gives $\ll x \log\log x/(\log x)^3$ for the number of p in consideration.

The contributions from both cases are $o(\#\mathcal{P}_2(x))$. So for sufficiently large x, we can find $p \in \mathcal{P}_2(x)$ satisfying

$$\omega^*(n(p-1)/2) = \omega^*(n) + 1.$$

The densities $\delta_k(\omega^*)$

Table 1: Exact counts of level sets for $k < 12$

k	10^4	10^6	10^8	10^{10}	$\approx \delta_k$
1	5,000	500,000	50,000,000	5,000,000,000	.5
2	834	77,696	7,436,825	720,726,912	.070
3	965	91,602	8,826,498	859,002,140	.084
4	877	79,986	7,691,971	748,412,490	.074
5	612	59,518	5,684,323	555,900,984	.055
6	456	40,641	4,031,009	401,146,301	.040
7	287	29,565	3,016,881	300,330,932	.030
8	202	23,190	2,324,769	233,611,502	.023
9	153	17,914	1,800,298	182,793,491	.018
10	159	13,899	1,401,307	144,740,573	.015
11	103	10,487	1,131,836	118,302,267	.012
≥ 12	352	55,682	6,654,283	735,032,408	

The largest values of k encountered here up to the various bounds: 10^4: 28, 10^6: 86, 10^8: 247, 10^{10}: 618. Perhaps the densities δ_k are monotone for $k \geq 3$.

The densities $\delta_k(\omega^*)$

We have seen that $\delta_k(\omega) = \delta_k(\tau) = 0$ for every fixed $k \in \mathbb{N}$. Consequently, the densities of the tails $\{n \in \mathbb{N} \colon \omega(n) > k\}$ and $\{n \in \mathbb{N} \colon \tau(n) > k\}$ are both equal to 1.

The densities $\delta_k(\omega^*)$

We have seen that $\delta_k(\omega) = \delta_k(\tau) = 0$ for every fixed $k \in \mathbb{N}$. Consequently, the densities of the tails $\{n \in \mathbb{N} \colon \omega(n) > k\}$ and $\{n \in \mathbb{N} \colon \tau(n) > k\}$ are both equal to 1. But this is not the case for ω^*.

Theorem 2 (F.–Pomerance, 2024)

For $x, y \geq 1$, let $N(x,y) := \#\{n \leq x \colon \omega^*(n) \geq y\}$. Then there exists a suitable constant $c > 0$ such that for all $x \geq 1$ and all sufficiently large y,

$$\left\lfloor \frac{x}{y^{c \log\log y}} \right\rfloor \leq N(x,y) \ll \frac{x \log y}{y}.$$

The lower bound follows from the result of Adleman, Pomerance and Rumely (1983) on the maximal order of ω^*, while the proof of the upper bound makes use of a theorem due to McNew, Pollack and Pomerance (2017), which asserts that the number of $n \leq x$ with a shifted prime divisor $> y$ is $O(x/(\log y)^{\eta+o(1)})$, where $\eta = 1 - (1 + \log\log 2)/\log 2$ is the Erdős–Ford–Tenenbaum constant.

Bernoulli numbers sharing the same fractional part

In our proof of Theorem 1, we used a result of Erdős and Wagstaff (1980) concerning the density $\delta(\langle n\rangle)$ of $\langle n\rangle$ for a given $n \in \mathbb{N}$, where

$$\begin{aligned}\langle n\rangle &:= \#\{m \in \mathbb{N}\colon B_m \equiv B_n \pmod 1\}\\ &= \#\{m \in \mathbb{N}\colon (p-1) \mid m \Leftrightarrow (p-1) \mid n\}. \quad \text{(von Staudt–Clausen)}\end{aligned}$$

Note that $\langle 1\rangle = \mathcal{L}_1 = \mathbb{N} \setminus 2\mathbb{N}$, so that $\delta(\langle n\rangle) = 1/2$ for odd n. Erdős and Wagstaff showed that $\delta(\langle n\rangle)$ exists and is positive for every $n \in \mathbb{N}$. They also observed that if $n = \min\langle n\rangle$, then $\delta(\langle n\rangle) < 1/n$. In this case, they asked for a positive lower bound for $\delta(\langle n\rangle)$.

Theorem 3 (F.–Pomerance, 2024)

Let $n \in 2\mathbb{N}$ *be such that* $n = \min\langle n\rangle$. *Then*

$$\delta(\langle n\rangle) \geq \frac{1}{n^{O(\tau(n))}}.$$

The moments of ω^*

For any arithmetic function f, we denote by $M_k(x; f)$ the *kth moment* of f for each $k \in \mathbb{N}$. That is,

$$M_k(x; f) := \frac{1}{x} \sum_{n \le x} f(n)^k.$$

The moments of ω^*

For any arithmetic function f, we denote by $M_k(x; f)$ the *kth moment* of f for each $k \in \mathbb{N}$. That is,

$$M_k(x; f) := \frac{1}{x} \sum_{n \leq x} f(n)^k.$$

For every fixed $k \in \mathbb{N}$, we have

$$M_k(x; \omega) \sim (\log \log x)^k,$$
$$M_k(x; \tau) \sim a_k (\log x)^{2^k - 1},$$

where

$$a_k := \frac{1}{(2^k - 1)!} \prod_p \left(1 - \frac{1}{p}\right)^{2^k} \sum_{\nu \geq 0} \frac{(\nu + 1)^k}{p^\nu}.$$

The moments of ω^*

Prachar (1955) showed $M_1(x;\omega^*) \sim \log\log x$, by observing that

$$\sum_{n\le x}\omega^*(n) = \sum_{n\le x}\sum_{p-1|n} 1 = \sum_{p\le x+1}\left\lfloor \frac{x}{p-1}\right\rfloor = x\sum_{p\le x}\frac{1}{p-1} + O\left(\frac{x}{\log x}\right).$$

He also proved $M_2(x;\omega^*) = O((\log x)^2)$, which was improved to $O(\log x)$ by Murty and Murty (2021), who also showed $M_2(x;\omega^*) \gg (\log\log x)^3$ and conjectured $M_2(x;\omega^*) \sim C\log x$ for some constant $C > 0$. Ding (2023) obtained the order matching lower bound $M_2(x;\omega^*) \gg \log x$.

In general,

$$M_k(x;\omega^*) = \frac{1}{x}\sum_{n\le x}\omega^*(n)^k = \frac{1}{x}\sum_{[p_1-1,\ldots,p_k-1]\le x}\left\lfloor \frac{x}{[p_1-1,\ldots,p_k-1]}\right\rfloor.$$

The moments of ω^*

Erdős and Prachar (1955) showed

$$S_2(x) := \sum_{[p-1,q-1]\le x} 1 = O(x),$$

which allows us to write

$$M_2(x;\omega^*) = \frac{1}{x}\sum_{[p-1,q-1]\le x}\left\lfloor \frac{x}{[p-1,q-1]}\right\rfloor = \sum_{[p-1,q-1]\le x}\frac{1}{[p-1,q-1]} + O(1).$$

The upper bound $M_2(x;\omega^*) = O(\log x)$ follows easily by partial summation.

The moments of ω^*

Erdős and Prachar (1955) showed

$$S_2(x) := \sum_{[p-1,q-1]\le x} 1 = O(x),$$

which allows us to write

$$M_2(x;\omega^*) = \frac{1}{x}\sum_{[p-1,q-1]\le x}\left\lfloor \frac{x}{[p-1,q-1]}\right\rfloor = \sum_{[p-1,q-1]\le x}\frac{1}{[p-1,q-1]} + O(1).$$

The upper bound $M_2(x;\omega^*) = O(\log x)$ follows easily by partial summation.

Theorem 4 (F.–Pomerance, 2024)

We have $M_3(x;\omega^*) \asymp (\log x)^4$ *for all* $x \ge 2$.

Conjecture 1 (F.–Pomerance, 2024)

For every $k \ge 2$, $M_k(x;\omega^*) \sim C_k(\log x)^{2^k-k-1}$, *where* $C_k > 0$ *is constant.*

The constant C_2

Under the Elliott–Halberstam conjecture, Ding, Guo, and Zhang (2023) deduced that $C_2 = 2\zeta(2)\zeta(3)/\zeta(6) \approx 3.88719$. However, an error found in their paper (inherited from Murty and Murty (2021)) by Pomerance and I shows that this value is probably incorrect.

Moreover, numerical computations seem to suggest $C_2 \approx 3.2$.

The constant C_2

Under the Elliott–Halberstam conjecture, Ding, Guo, and Zhang (2023) deduced that $C_2 = 2\zeta(2)\zeta(3)/\zeta(6) \approx 3.88719$. However, an error found in their paper (inherited from Murty and Murty (2021)) by Pomerance and I shows that this value is probably incorrect.

Moreover, numerical computations seem to suggest $C_2 \approx 3.2$.

Conjecture 2 (F., 2025)

We have

$$C_2 = \frac{\zeta(2)^2\zeta(3)}{\zeta(6)} \approx 3.19709.$$

This conjecture is suggested by a heuristic based on the Hardy–Littlewood conjecture on the infinitude of prime pairs $p = an + 1$ and $q = bn + 1$, where $1 \leq a < b$.

The constant C_2

Table 2: Numerical values of $M_2(10^k;\omega^*)$ and $S_2(10^k;\omega^*)$

k	$M_2(10^k)$	$S_2(10^k)$	$A(10^k)$	$B(10^k)$
2	9.71	2.42	9.34061	2.5028
3	15.530	2.624	15.4058	2.7342
4	21.9128	2.8175	21.8477	2.8499
5	28.49311	2.88636	28.4958	2.9193
6	35.261891	2.950910	35.2745	2.9656
7	42.1296839	2.9923851	42.1432	2.9987
8	49.07181351	3.02166709	49.0779	3.0235
9	56.067311859	3.043042188	56.0629	3.0428
10	63.1033824202	3.0595625181	63.0876	3.0582

The M_2 values fits nicely with $A(x) := C_2(\log x - \log\log x) - 1/2$, and the S_2 values may fit with $B(x) := C_2(1 - 1/\log x)$.

The shifted-prime divisor function over shifted primes

Theorem 5 (F., 2025)

For any fixed $a, b \in \mathbb{Z} \setminus \{0\}$, we have

$$\frac{1}{\pi(x)} \sum_{b<q\leq x} \omega_a^*(q-b) = C_{a,b} \log\log x + O\left(1\right),$$

where $C_{a,b} \geq 0$ is an explicit constant.

Theorem 6 (F., 2025)

For any fixed $a, b \in \mathbb{Z} \setminus \{0\}$ such that $2 \mid a$ or $2 \nmid b$, we have

$$\frac{1}{\pi(x)} \sum_{b<q\leq x} \omega_a^*(q-b)^2 \asymp \log x.$$

A generalization of Erdős–Prachar

The treatment of the second moment requires upper bounding

$$\sum_{\substack{[p-a,q-b]\le x\\ p>a,q>b}} f([p-a,q-b]),$$

which may be viewed as a two-dimensional analogue of

$$\sum_{a<p\le x+a} f(p-a),$$

where $f:\mathbb{N}\to\mathbb{R}_{\ge 0}$ is a "nice" multiplicative function.

Erdős and Prachar (1955) showed

$$\sum_{[p-1,q-1]\le x} 1 = O(x).$$

A generalization of Erdős–Prachar

For any $A_1 > 0$ and $A_2 \colon \mathbb{R}_{>0} \to \mathbb{R}_{>0}$, denote by $\mathscr{M}(A_1, A_2)$ the collection of multiplicative functions $f \colon \mathbb{N} \to \mathbb{R}_{\geq 0}$ satisfying:

1. $f(n) \leq A_1^{\Omega(n)}$ for all $n \in \mathbb{N}$.
2. $\forall \epsilon > 0$, $f(n) \leq A_2(\epsilon) n^{\epsilon}$ for all $n \in \mathbb{N}$.

Theorem 7 (F., 2025)

Let $a, b \in \mathbb{Z} \setminus \{0\}$, $A_1 > 0$, $A_2 \colon \mathbb{R}_{>0} \to \mathbb{R}_{>0}$, *and* $f \in \mathscr{M}(A_1, A_2)$. *Then*

$$\sum_{\substack{[p-a, q-b] \leq x \\ p > a, q > b}} f([p-a, q-b]) \ll_{a,b,A_1,A_2} \frac{x}{(\log x)^2} E_f(x) \int_2^x \frac{E_f(t)^2}{t(\log t)^2}\, dt$$

for all $x \geq 2$, *where*

$$E_f(x) := \exp\left(\sum_{p \leq x} \frac{f(p)}{p}\right).$$

The shifted-prime divisor function over shifted primes

For any $b \in \mathbb{Z} \setminus \{0\}$, let $N_b(x, y) := \#\{b < q \leq x : \omega^*(q-b) \geq y\}$.

Theorem 8 (F., 2025)

Fixing any $b \in \mathbb{Z} \setminus 2\mathbb{Z}$, there are constants $c_1, c_2 > 0$ such that

$$\frac{\pi(x)}{y^{c_1 \log\log y}} < N_b(x, y) \ll \frac{\pi(x) \log y}{y}$$

for all sufficiently large x and $y \leq x^{c_2/\log\log x}$.

The proof of Theorem 8 uses a slightly upgraded version of the result of Adleman, Pomerance and Rumely (1983) on the maximal order of ω^* and a bound on the number of shifted primes with a large shifted prime divisor due to Luca, Pizarro-Madariaga, and Pomerance (2014).

Shifted primes possessing a large shifted-prime divisor

McNew, Pollack and Pomerance (2017) showed that the number of $n \le x$ with a shifted prime divisor $q-1>y$ is

$$\ll \frac{x}{(\log y)^{\eta}\sqrt{\log\log y}},$$

where

$$\eta := 1 - \frac{1+\log\log 2}{\log 2} = 0.0860713...$$

is the Erdős–Tenenbaum–Ford constant. This makes more precise the bound $\ll x/(\log y)^c$ for some $c>0$ due to Erdős and Wagstaff (1980). Ford (2017) further refined these results for y in various ranges.

Luca, Pizarro-Madariaga, Pomerance (2014) studied the shifted-prime analogue, proving that for any $u \in \mathbb{N}$ and $v \in \mathbb{Z}$, there is a constant $c = c(u,v) > 0$ such that for $x, y \ge 3$, the number of $p \le x$ such that $up+v$ has a shifted-prime divisor $q-1>y$ with $q \ne p$ is

$$\ll_{u,v} \frac{\pi(x)}{(\log y)^c}.$$

Shifted primes possessing a large shifted-prime divisor

Theorem 9 (F., 2025+)

Let $a \in \mathbb{Z} \setminus \{0\}$, $u \in \mathbb{N}$ *and* $v \in \mathbb{Z} \setminus \{-au\}$. *The number of primes* $p \leq x$ *such that* $up + v$ *has a shifted-prime divisor* $q - a > y$ *is*

$$\ll_{a,u,v} \frac{\pi(x)}{(\log y)^{\eta}\sqrt{\log\log y}}$$

for all $x, y \geq 3$. *In addition, if* $3 \leq y \leq x/2$, *then the count is*

$$\ll_{a,u,v} \frac{\pi(x)\log(x/y)}{\log x}.$$

The proof of Theorem 9 is based on a general Hardy–Ramanujan type inequality for the count of numbers in a sifted set with a prescribed number of prime factors (F., 2025+).

A Hardy–Ramanujan inequality for sifted sets

Let $f\colon \mathbb{N} \to \mathbb{R}_{\geq 0}$ be a "nice" multiplicative function, and let $\mathcal{S}$ be the set of integers $n \in [1, x]$ which avoid a subset $\mathcal{E}_p \subseteq (\mathbb{Z}/p\mathbb{Z})^\times$ of $\nu(p) \ll 1$ reduced residue classes modulo p for every prime p. Then

$$\sum_{\substack{n \in \mathcal{S} \\ \omega/\Omega(n) = k}} f(n) \ll \frac{x M_f(x)^{k-1}}{(k-1)! \log x} \prod_{p \leq x} \left(1 - \frac{\nu(p)}{p}\right)$$

uniformly for $1 \leq k \leq c_0 M_f(x)$, where $c_0 > 0$ is a suitable constant, and

$$M_f(x) := \sum_{p \leq x} \frac{f(p)}{p}.$$

Pollack (2020) proved similar results for ω and all $k \in \mathbb{N}$ when $\mathcal{S} = [1, x]$.

Shifted primes in the image of λ

Recall the Carmichael λ-function $\lambda(n) = \mathrm{Exp}(\mathbb{Z}/n\mathbb{Z})^\times$:

$$\lambda(p^v) = \begin{cases} \frac{1}{2}\varphi(p^v), & \text{if } p = 2 \text{ and } v \geq 3, \\ \varphi(p^v), & \text{otherwise,} \end{cases}$$

and $\lambda(n) = \mathrm{lcm}\{\lambda(p^v) \colon p^v \parallel n\}$.

Luca and Pomerance (2013) proved that

$$\#(\lambda(\mathbb{N}) \cap [1, x]) \leq \frac{x}{(\log x)^{\eta + o(1)}},$$

and the order matching lower bound was furnished by Ford, Luca, and Pomerance (2014).

Shifted primes in the image of λ

Corollary 10

Given any $u \in \mathbb{N}$ *and* $v \in \mathbb{Z} \setminus \{-u\}$, *we have*

$$\#((u\mathbb{P}+v) \cap \lambda(\mathbb{N}) \cap [1,x]) \le \frac{\pi(x)}{(\log x)^{\eta + o_{u,v}(1)}}$$

for $x \ge 3$. *On the other hand, we have*

$$\#((u\mathbb{P}-u) \cap \lambda(\mathbb{N}) \cap [1,x]) \asymp_u \pi(x)$$

for sufficiently large x.

It seems natural to conjecture that for any fixed $u \in \mathbb{N}$ and $v \in \mathbb{Z} \setminus \{-u\}$,

$$\#((u\mathbb{P}+v) \cap \lambda(\mathbb{N}) \cap [1,x]) = \frac{\pi(x)}{(\log x)^{\eta + o(1)}}.$$

Happy Birthday, Carl and Melvyn!