Estimating the Number of Congruence Monoid Primes and Gaussian Primes

Rohan Sinha, Ian Kim, Ryan Diehl, William Gasarch
Johnathan Cai

August 25, 2025

Abstract

The Prime Number Theorem is a well-known asymptotic estimate for the number of primes. It states that the number of primes $\leq$ to a given number x is approximately $\frac{x}{\ln(x)}$. In this paper, we investigate the distribution of primes for congruence monoids and the circle of Gaussian integers in $\mathbb{Z}[i]$. We develop computational methods to count primes in both cases and compare their growth rates with the classical logarithmic model. Our results provide empirical evidence on the degree to which these primes follow $\frac{x}{\ln(x)}$, and where significant deviations occur.

Keywords: Prime Number Theorem, Gaussian Integers, Circles, and Primes.

1 Introduction

In 1896, Jacques Hadamard and Charles-Jean de la Vallée Poussin both independently discovered that the number of primes $\leq x$ was roughly $\frac{x}{\ln(x)}$ using complex analysis. This was built off of earlier work done by Pafnuty Chebyshev in the 1850s. This equation could be multiplied by any number x to determine the number of primes $\leq$ to x. The equation has been written as $\pi(x)$. Later proofs have been created for the Prime Number Theorem by

Paul Erdős and Atle Selberg in 1948. Their proof is elementary, only using calculus, hence why they reproved it.

In Section 2 we present the Congruence Monoid primes, Gaussian primes, and other important definitions. In Section 3 we present models for estimating the number of primes in the congruence monoid of 1 $\pmod{d}$ based on the Prime Number Theorem and also analyze the data surrounding it. In Section 4, we shift to Gaussian primes where we estimate the number of Gaussian primes within a Circle of radius r using a different model and also analyze its data. In section 5, we compare both cases to the classical logarithmic model and explain the differences and limitations. In Section 6, we present some open problems.

2 Key Definitions

Def 2.1 [Prime] Let $D \subseteq \mathbb{N}$. A *prime* in D is a number $p \in D$ such that $p > 1$ and the only positive divisors of p that lie in D are 1 and p itself.

Def 2.2 [Unit] An element $u \in D$ is called a *unit* (with respect to multiplication in D) if there exists $v \in D$ such that $u \cdot v = v \cdot u = 1$.

Def 2.3 [Irreducible] Let element $r \in D$ is called *irreducible* in D if r is not a unit of D and whenever $r = a \cdot b$ with $a, b \in D$, then at least one of a or b is a unit in D.

Def 2.4 [Congruence Monoid Prime] Let $d \in \mathbb{N}$ with $d \geq 2$. Define the set

$$A = \{n \in \mathbb{N} \mid n \equiv 1 \pmod{d}\}.$$

An element $p \in A$ is called a *congruence monoid prime* if whenever $p = ab$ for some $a, b \in A$, then either $a = 1$ or $b = 1$. Factorizations involving elements outside A are not considered.

Def 2.5 [Congruence Monoid Unit] An element $p \in A$ is called a *congruence monoid unit* if there exists $v \in D$ such that $u \cdot v = v \cdot u = 1$. The only *congruence monoid unit* is 1.

Def 2.6 [Gaussian Integer] A *Gaussian integer* is a complex number of the form $a + bi$, where $a, b \in \mathbb{Z}$. The set of all Gaussian integers is denoted by $\mathbb{Z}[i]$.

Def 2.7 [Gaussian Prime] A *Gaussian integer* $\pi \in \mathbb{Z}[i]$ is a *Gaussian prime* if it is nonzero, not a unit (i.e., not ± 1 or $\pm i$), and whenever $\pi = \alpha\beta$ for $\alpha, \beta \in \mathbb{Z}[i]$, then α or β is a unit, which means it is the same as a Gaussian irreducible. That is, when π is irreducible in $\mathbb{Z}[i]$.

Def 2.8 [Gaussian Unit] A *Gaussian integer* $\pi \in \mathbb{Z}[i]$ is a *Gaussian unit* if it can be multiplied by another *Gaussian integer* to equal 1.

Def 2.9 [Norm of a Gaussian Integer] For $z = a + bi \in \mathbb{Z}[i]$, the *norm* of z is defined as

$$N(z) = a^2 + b^2.$$

Def 2.10 [Norm Circle in $\mathbb{C}$] For a fixed $r \in \mathbb{N}$, the *norm circle* of radius r in the complex plane is the set of all complex numbers $z = a + bi \in \mathbb{Z}[i]$ such that the norm $N(z) = \sqrt{a^2 + b^2} \leq r$. Geometrically, these points lie within and on the circle centered at the origin with radius r.

3 Congruence Monoid Prime Estimation

Recall the set from Def 2.4

$$A = \{n \in \mathbb{N} \mid n \equiv 1 \pmod{d}\}.$$

Let $\pi_d(x)$ denote the number of primes $\leq x$ that lie in A, i.e.,

$$\pi_d(x) = \#\{p \leq x \mid p \in A \text{ and } p \text{ prime}\}.$$

An estimate for $\pi_d(x)$, is given by:

$$E_d(x) = \frac{x}{d(\log x)^{\ 1/d}}.$$

This formula modifies the classical Prime Number Theorem to the congruence monoid context, accounting for the arithmetic constraint $n \equiv 1 \pmod{d}$.

The exponent $\frac{1}{d}$ and the d term in the denominator were chosen to balance the sparser distribution of primes in A against the growth of x and were then verified empirically.

To evaluate the fit between the empirical count $\pi_d(x)$ and the estimation $E_d(x)$, the following normalized accuracy ratio is used:

$$R_d(x) = \frac{\pi_d(x)}{E_d(x)}.$$

A value of $R_d(x) \approx 1$ indicates strong alignment between empirical and estimated counts.

The table below displays the accuracy of the estimation across several values of d for primes $\leq x = 10^4$. The mean absolute percentage deviation (MAPE) measures the accuracy of a forecasting model, which in this case is $E_d(x)$. The corresponding graphs provide a visual comparison of $\pi_d(x)$ and $E_d(x)$ over the full range of x for a few values of d from the table.

d	Largest Prime	Actual Count	Estimate	R_d	$\lvert R_d - 1\rvert$	MAPE (%)
3	10000	1380	1590.21	0.86781	0.13219	9.05
5	9996	1210	1282.34	0.94358	0.05642	3.81
7	9997	1009	1039.97	0.97022	0.02978	2.45
9	10000	851	868.19	0.98020	0.01980	2.28
11	10000	745	742.93	1.00279	0.00279	2.88
13	9998	653	648.33	1.00720	0.00720	3.10
21	9997	438	428.29	1.02268	0.02268	3.88
50	9951	196	190.38	1.02953	0.02953	3.03

Table 1: Comparison of Actual and Estimated $\mathrm{D_d}$-Prime Counts up to 10^4

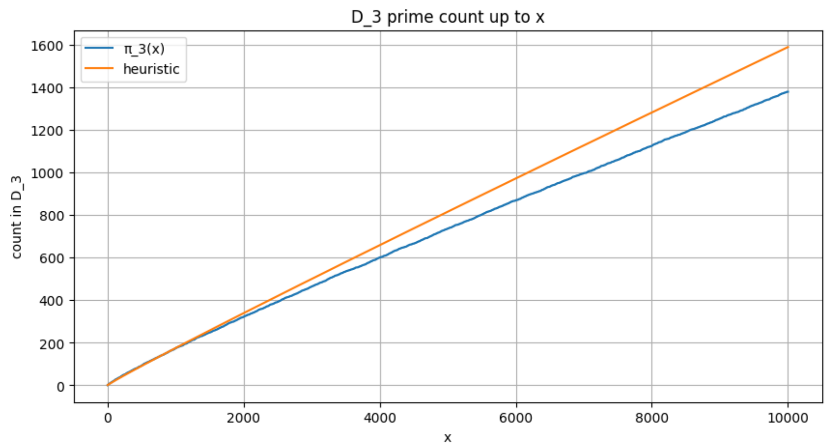

Figure 1: Actual prime count $\pi_3(x)$ (blue) versus the estimate $E_3(x)$ (orange) for $d = 3$.

The estimation very minorly underestimates until $x \approx 800$, then increasingly starts to overestimate.

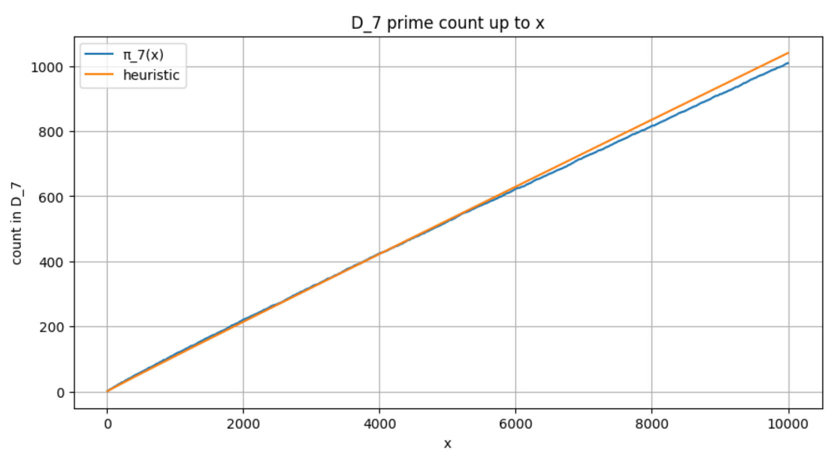

Figure 2: Actual prime count $\pi_7(x)$ (blue) versus the estimate $E_7(x)$ (orange) for $d = 7$.

Similar to figure 1, the estimate very minorly underestimates until $x \approx 4100$ and then increasingly starts to overestimate.

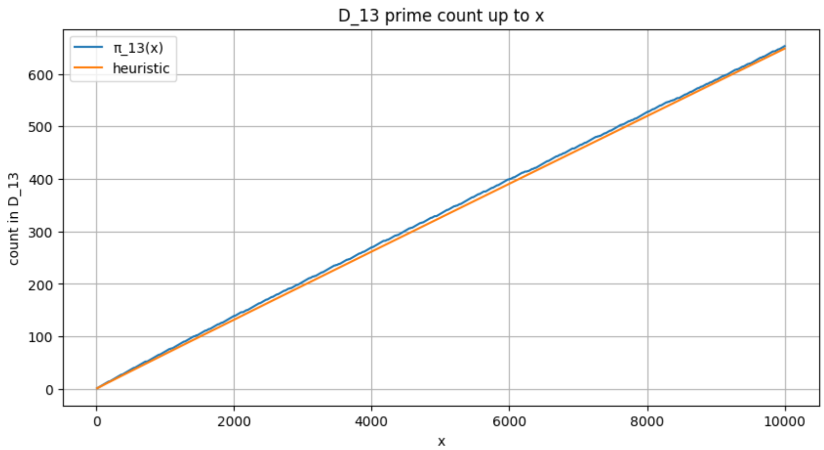

Figure 3: Actual prime count $\pi_{13}(x)$ (blue) versus the estimate $E_{13}(x)$ (orange) for $d = 13$.

Same phenomenon described above except at $x \approx 13800$ (not shown in graph).

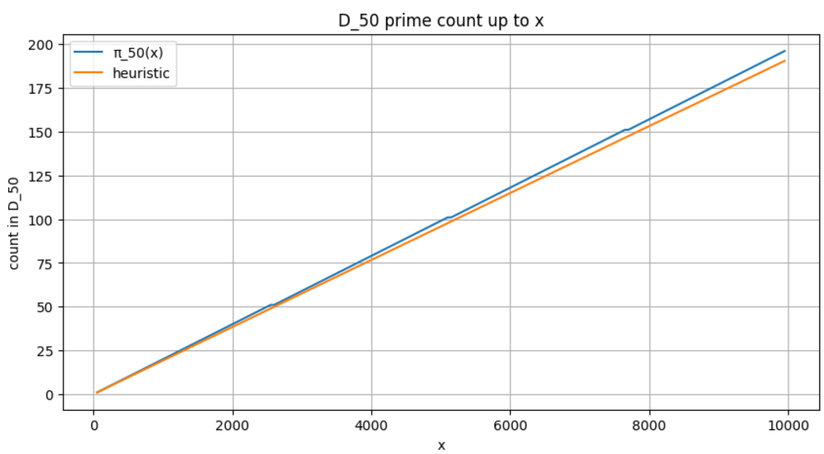

Figure 4: Actual prime count $\pi_{50}(x)$ (blue) versus the estimate $E_{50}(x)$ (orange) for $d = 50$ up to $x = 10\,000$.

Same phenomenon described above except at $x \approx 330,000$ (not shown in graph).

Unlike the Prime Number Theorem, where the estimation becomes more accurate as x grows (in fact, becomes perfect as x approaches infinity), the accuracy of our estimation is not as straightforward. The estimation becomes increasingly accurate up to a certain value of x (almost exact) and then diverges from the actual count.

4 Gaussian Prime Estimation

Recall we are counting the number of *Gaussian primes* within and on the *norm circle* in $\mathbb{Z}[i]$ with a radius r. That is, all $z = a + bi \in \mathbb{Z}[i]$ whose norm $N(z) = \sqrt{a^2 + b^2}$ satisfies $N(z) \leq r$. Using the norm circle provides a clear and finite boundary, making it possible to study the distribution of Gaussian primes up to a specific size, analogous to counting up to x in section 3 and for the classical PNT.

The number of Gaussian primes in and on the norm circle is π_G. We empirically found an estimate for π_G, $E_G(\text{r}) = \dfrac{4r}{\ln(r)}$. This is likely due to the fact that there are 4 units in the Gaussian integer domain compared to 1 in the natural number domain.

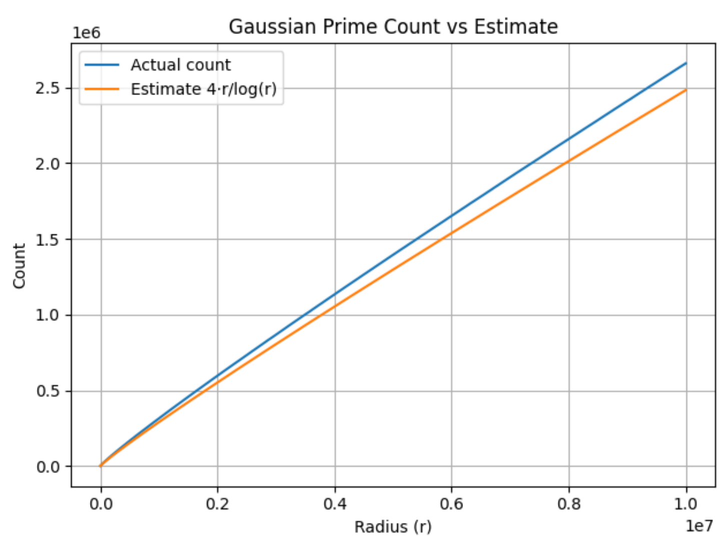

Figure 5: Actual Gaussian prime count for $0 < r^2 \leq 10^7$ (blue) versus the the estimate $E_G(r)$ (orange).

Radius (r)	MAPE (%)
10^3	14.95
10^4	12.63
10^5	10.31
10^6	8.50
10^7	7.21

Table 2: Mean absolute percentage deviation (MAPE) of the estimate $\pi_G(r)$ at various radii.

Since our estimate $E_G(\mathrm{r}) = \dfrac{4r}{\ln(r)}$ was shown to be accurate as the radius increased, future research that could rigorously prove our suggested estimate for Gaussian primes would be beneficial.

5 Conclusion

We analyzed primes in congruence monoids and Gaussian integers. For monoids of the form $n \equiv 1 \pmod{d}$, we proposed the estimate $E_d(x) = \frac{x}{d(\log x)^{1/d}}$, which fits well for small x but diverges as x grows. Its accuracy is not as straightforward as the classical PNT rather gets maximized at a certain point for each specific value of d. The value of x grew as d grew as seen in the graphed examples. For Gaussian integers, we found the classical model undercounts primes and adjusted it with a scaling factor $C \approx 4$ for an accurate fit. Just like the classical PNT, the accuracy of this estimate also increases as x increases. Both cases show prime-like elements follow modified versions of the prime number theorem, but need domain-specific corrections.

6 Open Problems

1. Rigorously prove the suggested estimate for congruence monoid primes.
2. Solve for the intersection point between the estimate and the actual number of congruence monoid primes.
3. Rigorously prove the suggested estimate for Gaussian primes.