[Math Seminar] The Parity Problem in Sieve Theory

Connor Li, csl2192

Spring 2024

Important Resources

- **Email:** csl2192@columbia.edu
- **Link to Class Webpage:** Click Here
- **[Johnny] Introduction to Sieves:** Click Here
- **Class Textbook:** Additive Number Theory
- **Brun's Sieve Reference Material (1):** Click Here
- **Buun's Sieve Reference Material (2):** Click Here
- **Selberg's Sieve Reference Material:** Click Here
- **The Large Sieve Reference Material:** Click Here

Contents

1 Review of Sieves

1.1 Introduction

Sieve methods are pivotal in the realm of number theory for their capacity to discern integers that exhibit particular arithmetic properties, such as primality. Specifically, they are used to answer a core question in number theory related to counting the number of primes from any given set of integers.

At a larger scale, sieves work by a process of elimination or "exclusion". In the context of prime numbers, this means that we start with the entire set of desired integers and slowly filter out the composite numbers (multiples of some prime) until we are left with a set of only primes.

In fact, the versatility of sieves allows you to extend this logic in order to also provide upper and lower bounds on certain progressions of primes (i.e. sequences of twin primes where p and $p+2$ are both prime), which we will not cover explicitly in this paper (but there are a lot of resources online for you to delve into). However, to explain how sieves work and their relation to the parity problem, let's first consider the most elementary problem of counting the number of primes in the interval $[N, 2N]$ where $N \in \mathbb{Z}^+$ (the set of positive integers).

1.2 The Counting Prime Problem

If the ultimate goal is to "filter out composite numbers" using our sieve, we need to be able to count sets of $n \in [N, 2N]$ where $n \equiv a \bmod q$. Specifically, if $a = 0$, we are interested in the set of integers where n is a multiple of some integer q. By a simple counting argument, it should be obvious that

$$|\{n \in [N, 2N] \ : \ n \equiv a \bmod q\}| = \frac{N}{q} + \mathcal{O}(1)$$

Building off that, let's consider the problem of counting the set of integers coprime to 2 in the interval $[N, 2N]$. Specifically, the set of coprime integers to 2 can be calculated by subtracting the integers $\equiv 0 \bmod 2$ from the total number of integers in the interval $[N, 2N]$. Thus, we have the following result for the cardinality of our desired set.

$$\begin{aligned}
|\{n \in [N, 2N] \ : \ n \text{ is coprime to } 2\}| &= |\{n \in [N, 2N]\}| - |\{n \in [N, 2N] : n \equiv 0 \bmod 2\}| \\
&= [N + \mathcal{O}(1)] - \left[\frac{N}{2} + \mathcal{O}(1)\right] \\
&= \frac{N}{2} + \mathcal{O}(1)
\end{aligned}$$

If we further extend this notion, we can then count the number of integers coprime to 2 and 3 using combinatorial logic (inclusion-exclusion principle). If we label the desired set N_0, we have that

$$\begin{aligned}
N_0 &= |\{n \in [N, 2N]\}| - |\{n \in [N, 2N] : n \equiv 0 \bmod 2\}| - |\{n \in [N, 2N] : n \equiv 0 \bmod 3\}| + |\{n \in [N, 2N] : n \equiv 0 \bmod 6\}| \\
&= [N + \mathcal{O}(1)] - \left[\frac{N}{2} + \mathcal{O}(1)\right] - \left[\frac{N}{3} + \mathcal{O}(1)\right] + \left[\frac{N}{6} + \mathcal{O}(1)\right] \\
&= \frac{N}{3} + \mathcal{O}(1)
\end{aligned}$$

Similar to the case where we consider the integers coprime to 2, we start with the entire set, subtracting the multiples of 2 and 3, and then adding back the multiples of 6 to account for the double counting. If we extend this to a larger and larger set of primes (i.e. numbers that are coprime to $2, 3, 5, 7, \ldots$), we can then use the sieve method to estimate the number of primes in the interval $[N, 2N]$.

1.3 Combinatorial Sieves

So, if this method above works, then why is the book on primes not closed? Well, it's because inclusion-exclusion blows up exponentially. In fact, as the set of primes with cardinality k grows, the number of terms in our inclusion-exclusion grows exponentially to 2^k. With an error term of $\mathcal{O}(1)$ for each term, the error term can - at worst - be $\mathcal{O}(2^k)$. In fact, after $k > \log N$ steps, our error term blows up to be so large that all results seem virtually meaningless.

Now, instead of getting a perfect result with a massive error term, what if we got an upper-or-lower bound? By simply truncating the sum at some point, we can get a bound that is more managable and meaningful. And although this was covered in my talk on Brun's sieve and its relation to twin primes, I think the problem is interesting and important to our discussion of sieves.

Specifically, if you enumerate the primes $P = \{p_1, p_2, p_3, \ldots, p_r\}$ and consider the some subset of those primes $I \subset P$, we can define the set $N(I)$ as the integers in the interval $[N, 2N]$ that are divisible by all primes in I. Then, we can use the sieve method described in Section 1.2 to count the number of integers not divisble by any of the primes in P, which we will label N_0. Finally, it is easy to see that if the sum truncates at an even r, then we have an upper bound.

$$N_0 \leq \sum_{k=0}^{r} (-1)^k \sum_{|I|=k} N(I) \qquad \text{if } r \text{ is even}$$

And if the sum truncates at an odd r, then we have an lower bound.

$$N_0 \geq \sum_{k=0}^{r} (-1)^k \sum_{|I|=k} N(I) \qquad \text{if } r \text{ is odd}$$

This type of logic is the basis for all combinatorial sieves.

1.4 Further Sieves

However, this is still is not good enough for our purposes. The "black and white" approach of combinatorial sieves, where numbers are either completely included or excluded based on their divisibility, is limited in scope. It's not nuanced enough for complex tasks such as estimating the distribution of primes within a specific range. In fact, this method tends to either overestimate or underestimate the count as it doesn't account for the subtleties of number distribution and the influence of factors such as prime gaps.

However, modern sieve theory has adjusted for this sublety by using sum of weight functions. At a higher level, these weight functions provide a more nuanced approach, allowing for partial contributions of terms in sums that more accurately reflect the number theoretic structures being studied. These partial contributions can be fine-tuned to minimize error terms and thus improve the accuracy of prime number estimates through more complex theorems (which we will exclude for the sake of brevity).

To show how these weight functions work, start with the basic equation where $1_A(n)$ is the indicator function of A.

$$|A| = \sum_{n \in [N, 2N]} 1_A(n)$$

If we carefully chose $c_d \in \mathbb{R}$ such that $1_A(n) \leq \sum_d c_d 1_{d|n}(n)$ for all $n \in [N, 2N]$, then we can rewrite our bound as follows.

$$|A| \leq N \sum_d \frac{c_d}{d} + \mathcal{O}\left(\sum_d |c_d|\right)$$

If we continue to add additional weights or include more residue classes in our summation, we can take this basic idea of weighted combinatorial sum and extend it to more complex problems like counting twin primes.

In terms of choosing weights, first notice that the choice of $c_d = \{0, \pm 1\}$ is the combinatorial sieve we discussed earlier. And, similar to the issues that we've seen in the above sieves, the main problem in choosing weights is to make sure that the c_d are chosen such that $\mathcal{O}\left(\sum_d |c_d|\right)$ doesn't swamp our main bounding term. Explicitly, we usually pick $c_d \leq N^\epsilon$ where N^ϵ is some very small power of N. This concludes our discussion of sieves!

2 The Parity Problem

2.1 Introduction

Now, the problem with sieves is something - originally introduced by Selberg - that prevents us from counting or lower bounding the primes themselves. So although sieves can provide good upper bounds, lower bounds, and even asymptotic approximations for “almost primes”, their inability to distinguish between integers with an odd or even number of prime factors - hence the term ”parity” - causes an oversight on the subtle arithmetic properties that would allow for our desired precise lower bounds on primes.

2.2 The Problem

Formally, the Parity Problem is stated as follows.

Definition: If A is a set whose elements are all products of an odd number of primes (or are all products of an even number of primes), then (without injecting additional ingredients), sieve theory is unable to provide non-trivial lower bounds on the size of A. Also, any upper bounds must be off from the truth by a factor of 2 or more.

In simpler terms, sieve theory is unable to distinguish between integers with an odd or even number of prime factors. This is because the combinatorial sieves we discussed earlier are not nuanced enough to account for the parity of the number of prime factors, thus called the “parity” problem.

So, sieve theory allows us to count almost primes (with even or odd number of prime factors) or count numbers with 6 or 7 prime factors, which can be counted by the Bombieri sieve. However, the parity problem is important because it directly implicates the idea of counting primes. Since primes are definitionally integers with odd number of prime factors (specifically 1), sieve theory is unable to provide particularly meaningful bounds on the number of exact primes (not almost primes) in a given interval. Similarly, we cannot use plain sieve theory to answer the question about counting semiprimes, which we are numbers with only 2 prime factors.

2.3 Example

2.3.1 Overview of The Selberg Problem

The most famous example of the parity problem was introduced by Selberg and later referenced by Cojocaru and Murty. Essentially, the problem is presented as follows.

Imagine you have some set A defined as the set of integers less than or equal to x such that it has no prime divisors $\leq x^{\frac{1}{2}}$ that also have an even number of prime factors. More formally,

$$A = \left\{ n \in [1, x] \;:\; n \neq 0 \bmod p,\ \forall p \leq x^{\frac{1}{2}} \text{ and } n \text{ has an even number of prime factors} \right\}$$

In the next section, we will prove the next proposition; but if we try to find the cardinality of set A, no matter what type of sieve we use (and any choice of weights for those sieves), the upper bound for this set is always the following.

$$|A| \leq \frac{(2 + \mathcal{O}(1))x}{\ln(x)}$$

However, this bound isn't good at all because if you think about this set logically, the cardinality of set $|A|$ should always be 0. This should be fairly obvious, but if some n has an even number of prime factors, at least one of them must be $\leq x^{\frac{1}{2}}$, which means that $|A|$ must be of cardinality 0. As you can see, in the case of only even prime factors, sieve methods are pretty much unable to generate any meaningful bound on the defined set A.

Similarly, take the same problem but only consider those numbers with an odd number of prime factors. So now, the set A is defined as

$$A = \left\{ n \in [1, x] \;:\; n \neq 0 \bmod p,\ \forall p \leq x^{\frac{1}{2}} \text{ and } n \text{ has an odd number of prime factors} \right\}$$

No matter what type of basic sieve we use and the weights we pair with said sieve (which weill will prove in the next section), the upper bound for this set is always as follows.

$$|A| \leq \frac{(2 + \mathcal{O}(1)) \cdot x}{\ln(x)}$$

However, this bound is terrible! If you think about this set outside of the concept of sieves, the elements of A are just the prime numbers from $(x^{\frac{1}{2}}, x]$, which we we can count using the PNT (prime number theorem). However, if we use sieve methods to estimate this set, we get a looser bound compared to the prime number theorem.

$$|A| \leq \underbrace{\frac{(1 + \mathcal{O}(1)) \cdot x}{\ln(x)}}_{\text{PNT}} \leq \underbrace{\frac{(2 + \mathcal{O}(1)) \cdot x}{\ln(x)}}_{\text{Sieve Methods}}$$

So as you can clearly see, the sieve method is unable to bound the set A and actually overestimates the upper bound on the second set by a factor of 2.

2.3.2 Formal Analysis of the Parity Problem

As promised, let's delve into specifics. To provide a more formal analysis of the parity problem, let's introduce the following Liouville function $\lambda(n)$.

$$\lambda(n) = \begin{cases} +1 & \text{if } n \text{ has an even number of prime factors} \\ -1 & \text{if } n \text{ has an odd number of prime factors} \end{cases}$$

Let's say that we want to count the set A such that A consists of all integers $n \in [N, 2N]$ such that n has an even number of prime factors. Using sieve methods described above, we can set up the following weighted divisor-sum bound using our indicator function such that

$$1_A(n) \geq \sum_d c_d 1_{d|n}(n)$$

However, we are only interested in the set where A has an even number of prime factors, so we multiply by the non-negative weight of $(1 + \lambda(n))$ so that the indicator function evalutes to 0 in the scenario where n has odd number of prime factors. This results in the following

$$1_A(n)(1 + \lambda(n)) \geq \sum_d c_d 1_{d|n}(n)(1 + \lambda(n))$$

Since $n \in [N, 2N]$, whenever $1_A(n) = 1$, we also know that $(1 + \lambda(n)) = (1 + (-1)) = 0$ which means that the summation across all possible n also evaluates to 0.

$$\sum_n 1_A(n)(1 + \lambda(n)) \geq \sum_n \sum_d c_d 1_{d|n}(n)(1 + \lambda(n))$$
$$0 \geq \sum_d c_d \frac{N}{d} + \cdots$$

If you can see, we can't improve on the trivial bound, which means that the sieve method doesn't tell us any particularly meaningful results.

Similarly, if we use the case where $1 - \lambda(n)$ to quantify the new set A which is the basically the same set except elements of A have an odd number of prime factors, then we get the following.

$$\sum_n 1_A(n)(1 - \lambda(n)) = |A| \implies 2|A| \geq |A|$$

And although the proof is somewhat more involved, the general idea is that $2 \geq 1 - \lambda(n)$, which lets us bound the set A in a non-meaningful way.

Ultimately, since all prime numbers have an odd number of prime factors, sieve methods are unable to provide non-trivial lower bounds on the number of primes in a given interval. And in the field of number theory, this is a very significant problem since the question of primes is central to the field and current research.

3 Overcoming the Parity Problem

3.1 Overview

However, not all hope is lost! The quest to count prime numbers and understand their distribution among integers has led to the development of sophisticated techniques in analytic and algebraic number theory. These techniques extend beyond the classical sieve theory, particularly when addressing complex forms such as quadratic and higher-degree polynomials.

3.2 Prime Number Theorem

A foundational result in the field is the Prime Number Theorem (PNT), which predicts the asymptotic distribution of primes. The PNT was initially proven using complex analysis methods by Hadamard and de la Vallée Poussin. A link of this proof is included here.

An alternative "elementary" proof, one that avoids complex analysis, was later provided by Erdős and Selberg. This proof utilizes the multiplicative structure of primes and almost primes—numbers with only a small number of prime factors. The idea here hinges on showing that the density of these almost primes mimics, to some extent, the density of prime numbers. However, this elementary approach faces limitations when applied to more complex scenarios, such as counting twin primes (pairs of primes that differ by two), where the product of such primes does not fall neatly into the established frameworks of almost primes. A link of this proof is included here.

3.3 Special Prime Counting

The work of Friedlander and Iwaniec marked a significant breakthrough in counting primes represented by specific polynomial forms. They demonstrated that there are infinitely many prime numbers of the form $a^2 + b^4$. This result was achieved through an intricate argument beginning with Vaughan's identity—an advanced tool in sieve theory that introduces an exact representation with a bilinear error term. This term, essentially capturing correlations with the Liouville function, required meticulous control through arithmetic manipulations, including factorization over the Gaussian integers. A crucial part of their analysis was understanding the interactions between the Möbius function and the Jacobi symbol, achieved using a variety of number-theoretic techniques.

This method was further adapted by Heath-Brown to prove the infinitude of primes of the form $a^3 + 2b^3$, and similar methods have been applied to other cubic forms by researchers such as Heath-Brown, Moroz, and Helfgott. These results generally hinge on representing the forms as norms over certain number fields, highlighting the deep connections between number theory and algebraic structures.

3.4 Almost Primes and Combinatorics

One strategy to overcome the parity problem involves the utilization of almost primes interlayed with combinatorial techniques to achieve lower bounds on certain prime progressions. Although this sounds daunting and may seem unclear at first, let's consider the following example.

Define P_2 as the set of all numbers in the interval $[N, 2N]$ that have exactly two prime factors and the set A as follows.

$$P_2 = \{n \in [N, 2N] \, : \, n, n+2, n+6 \in P_2\}$$

Now, suppose that you were able to get good lower bounds on the following sets.

$$\begin{aligned} A_1 &= \{n \in [N, 2N] \, : \, n \text{ prime}\} \\ A_2 &= \{n \in [N, 2N] \, : \, n+2 \text{ prime}\} \\ A_3 &= \{n \in [N, 2N] \, : \, n+6 \text{ prime}\} \end{aligned}$$

Finally, if you are able to count the set A such that $|A| < |A_1| + |A_2| + |A_3|$, then you can use the pigeonhole principle to deduce that there exists at least one number in the interval $[N, 2N]$ such that $n, n+2, n+6$ are all prime. This would imply that there are at least two primes in the triplet $(n, n+2, n+6)$, presenting a maximum prime gap of 6.

While the naive approach of directly using P_2-almost primes can offer some insights, further optimizations can be achieved. For example, replacing the condition that $n, n+2, n+6 \in P_2$ with a more nuanced condition can yield stronger results. This was done by Goldston, Yildirim, and Pintz (their paper is linked here) who were able to show that prime gaps $\in [N, 2N]$ can be as small as $\mathcal{O}(\log N)$ using a more refined version of the above method.

3.5 Future Research Development

Despite the parity problem, the field of number theory related to sieves continues to evolve. Researchers are actively exploring both broader applications of these existing sieve methods and entirely new approaches that may finally circumvent the limitations posed by the parity problem. The ongoing work promises not only deeper insights into the distribution of primes but also advancements in the tools of algebraic and analytic number theory itself. Specifically, this exploration into the counting of primes also impacts primes of special forms, which not only extends our understanding of prime distribution(s), but also continuously pushes the boundaries of mathematical research - offering glimpses into the profound interconnectedness of different mathematical domains.

4 Sources

- Tao, T. (2007, June 5). Open question: The parity problem in sieve theory. What's new. `https://terrytao.wordpress.com/2007/06/05/open-question-the-parity-problem-in-sieve-theory/`.
- Heath-Brown, D. R. (1982). A parity problem from sieve theory. Mathematika, 29(1), 1-6. `https://doi.org/10.1112/S0025579300012109`.
- Math 229: Analytic Number Theory. Illustration of the "parity problem" in Selberg's sieve: The case of Fq[t]. Math 229: Introduction to Analytic Number Theory. `https://people.math.harvard.edu/~elkies/M229.15/muff.pdf`.
- Friedlander, J., & Iwaniec, H. (2009). What Is... the Parity Phenomenon? Notices of the American Mathematical Society, 56(7), 817–818. `https://www.ams.org/notices/200907/rtx090700817p.pdf`.
- Friedlander, J., & Iwaniec, H. (1997). Using a Parity-Sensitive Sieve to Count Prime Values of a Polynomial. Proceedings of the National Academy of Sciences of the United States of America, 94(4), 1054–1058. `http://www.jstor.org/stable/41282`.
- Zagier, D. (1997). Newman's Short Proof of the Prime Number Theorem. The American Mathematical Monthly, 104(8), 705-708. Mathematical Association of America. Retrieved from `http://www.jstor.org/stable/2975232`.
- Goldfeld, D. (n.d.). THE ELEMENTARY PROOF OF THE PRIME NUMBER THEOREM: AN HISTORICAL PERSPECTIVE. Retrieved from `https://www.math.columbia.edu/~goldfeld/ErdosSelbergDispute.pdf`.
- Wikipedia contributors. (n.d.). Parity problem (sieve theory). In Wikipedia, The Free Encyclopedia. Retrieved from `https://en.wikipedia.org/wiki/Parity_problem_(sieve_theory)`.