[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, 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, as you will see later on, 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). However, to explain how sieves work and their relation to the parity problem, let's first consider the most basic 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," 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

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

Now, we can arrive at more interesting results like counting the set of integers coprime to 2 in the interval $[N, 2N]$. Applying the logic above, 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 the set.

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

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

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

Similar to the case with only coprimality to 2, we are taking 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 continue this principle to a set of larger and larger primes (i.e. numbers that are coprime to $2, 3, 5, 7, \ldots$), we can then use the sieve method to count 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.

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

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

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

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. 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 $1_A(n) \le \sum_d c_d 1_{d|n}(n)$ for all $n \in [N, 2N]$, then we can rewrite our bound as follows.

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

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 $c_d = \{0, \pm1\}$ 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 $c_d \le N^\epsilon$ 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.

3 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