Sieve Methods: Limitations, Parity, and Polynomials

Aditya Mittal

CCD: Dissertation
Mathematical Institute

September 15, 2026

Overview

1. The Principle of Sieve Methods
2. The Parity Problem
3. Overcoming Parity
4. Conclusion

The Principle of Sieve Methods

The Principle of Inclusion-Exclusion

- General problem of estimating sizes of sets
- Sift out "bad elements" from an ambient set and remain with only good elements
- More generally, let
  - $\mathcal{A} \subseteq \mathbb{N}$ finite subset (ambient set we sift from)
  - $\mathcal{P} \subseteq \mathbb{P}$ (the primes we sift out)
  - $z \in \mathbb{N}$ (an upper limit on how far we sift)
- We want to calculate

$$\mathcal{S}(\mathcal{A}, \mathcal{P}; z) = \{n \in \mathcal{A} : \forall p \in \mathcal{P} \ \ (p \mid n \Rightarrow p \geq z)\}$$

Basic Sieve Theory

- This divisibility criterion is quite general

Examples (Counting Primes)

Let $\mathcal{A} = \mathbb{N}_{\leq n}, \mathcal{P} = \mathbb{P}, z = \sqrt{n}$, then $\mathcal{S}(\mathcal{A}, \mathcal{P}; z) = \pi(n) - \pi(z)$

Examples (Twin Prime Conjecture)

Let $\mathcal{A} = \{n(n+2) : n \leq N\}, \mathcal{P} = \mathbb{P}, z = \sqrt{N+2}$, then $\mathcal{S}(\mathcal{A}, \mathcal{P}; z)$ is the number of twin primes in $[z, N]$.

- Let $\Pi = \prod\{p \in \mathcal{P} : p < z\}$, $\mathcal{A}_d = \{n \in \mathcal{A} : n \equiv 0 \bmod d\}$, then we recover inclusion-exclusion:

$$\mathcal{S}(\mathcal{A}, \mathcal{P}; z) = \sum_{d \mid \Pi} \mu(d) \# \mathcal{A}_d$$

Sieves in Different Settings: $\mathbb{F}_q[t]$

- Sieves operate on very general data $\rightarrow$ applies in general settings
- E.g. works in polynomial ring $\mathbb{F}_q[t]$. Let
  - $\mathcal{A} \subseteq \mathbb{F}_q[t]$ finite subset
  - $\mathcal{P} \subseteq \mathbb{P} = \{\text{monic irreducible polynomials } \mathfrak{p}\}$
  - $m \in \mathbb{N}$
- We can then calculate

$$\mathcal{S}(\mathcal{A}, \mathcal{P}; z) = \{f(t) \in \mathcal{A} : \forall \mathfrak{p}(t) \in \mathcal{P} \;\; (\mathfrak{p} \mid f \Rightarrow \deg \mathfrak{p} \geq m)\}$$

Examples (Twin Prime Conjecture)

Fix $K \in \mathbb{F}_q[t]$ with $\deg K < n$. Let $\mathcal{A} = \{f(f+K) : \deg f = n\}, \mathcal{P} = \mathbb{P}, m = n/2$, then $\mathcal{S}(\mathcal{A}, \mathcal{P}; z)$ is the number of degree n irreducible pairs $f, f+K$.

Example Bounds from Sieves

Examples (Counting Primes)

$$\pi(x) = \mathcal{S}(\mathcal{A}, \mathcal{P}; z) \leq (2 + o(1))\frac{x}{\log x}$$

$$\pi_q(n) = \mathcal{S}(\mathcal{A}; \mathcal{P}; m) \leq (2 + o(1))\frac{q^n}{n}$$

Examples (Twin Primes)

$$\mathcal{S}(\mathcal{A}, \mathcal{P}; z) \leq (C_2 + o(1))\frac{x}{(\log x)^2}$$

$$\mathcal{S}(\mathcal{A}; \mathcal{P}; m) \leq (C_K + o(1))\frac{q^n}{n^2}$$

The Parity Problem

The Parity Problem

- Let $p_1 \cdots p_k = \ell \mid \Pi$
- Let $n_1 = \ell \cdot q_1$, $n_2 = \ell \cdot q_1 q_2$ where $q_i \geq z$ prime
- Hence $(n_1, \Pi) = (n_2, \Pi)$ and $n_1 \in \mathcal{A}_d \iff n_2 \in \mathcal{A}_d$
- n_1 and n_2 look the same to the sieve, even though cofactors $q_1 \neq q_1 q_2$
- Importantly $\Omega(q_1) \neq \Omega(q_1 q_2)$
- **Given the same $\#\mathcal{A}_d$, sieves must produce the same outputs regardless of the parity of its elements**
- Problem for counting prime-/irreducible-related sets!

The Parity Problem

- Let $\mathcal{A} = \{x \leq n\}$
- Let $\lambda(n) = (-1)^{\Omega(n)}$ be the Liouville function
- $\mathcal{A}^{\pm} = \{n \in \mathcal{A} : \lambda(n) = \pm 1\}$
- $\sum_{n \leq x} \lambda(n) = o(x)$
- So $\mathcal{A}^{+}, \mathcal{A}^{-}$ have roughly same divisibility data i.e. $\#\mathcal{A}_d^{+} \approx \#\mathcal{A}_d^{-}$
- $\mathcal{A}_d = \mathcal{A}_d^{+} \cup \mathcal{A}_d^{-}$, and so $\#\mathcal{A}_d \approx 2\mathcal{A}_d^{-}$

The Parity Problem

$$\sum_{d|\Pi} \mu^*(d)\#\mathcal{A}_d = (2+o(1))\sum_{d|\Pi} \mu^*(d)\#\mathcal{A}_d^- \geq (2+o(1))\mathcal{S}(\mathcal{A}^-,\mathcal{P};x^{1/3}) = (2+o(1))\frac{x}{\log x}$$

$$\sum_{d|\Pi} \mu^*(d)\#\mathcal{A}_d = (2+o(1))\sum_{d|\Pi} \mu^*(d)\#\mathcal{A}_d^+ \leq (2+o(1))\mathcal{S}(\mathcal{A}^-,\mathcal{P};x^{1/2}) = 2+o(1)$$

- Primes are only contained in $\mathcal{A}^-$, but the sieve cannot distinguish from $\mathcal{A}^+$

The Parity Phenomenon

"If $\mathcal{A}$ 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 $\mathcal{A}$. Also, any upper bounds must be off from the truth by a factor of 2 or more" (Tao, 2007)

Overcoming Parity

What Additional Ingredients?

- Sieves in different settings pose different opportunities and challenges
- $\mathbb{Z}$ vs. $\mathbb{F}_q[t]$ have vastly different analytic properties
- **Can we leverage these to break past the parity problem?**
- Simple example from counting primes: we know the parity information well
- We know $\#\mathcal{A}_d^- \approx \frac{1}{2}\#\mathcal{A}_d$, so pre-processing the parity information (size, which) above gives the correct, tight upper bound
- For polynomials, this is genuinely an improvement on the sieve as we can show $\sum_{\deg N=d} \mu(N) = 0$ elementarily

Twin Prime Conjecture Strategies

- In $\mathbb{Z}$ (Chen):
  - Current: infinitely many $p, p+2$ with $\Omega(p+2) \leq 2$ (parity still an issue)
  - Formulate as $\mathcal{A} = \{p+2 : p \text{ prime}, p \leq x\}$ to cleanly separate the pair
  - Requires knowledge of distribution: Bombieri-Vinogradov theorem
  - Turns lower bound problem into upper bound problem using arithmetic relation
- In $\mathbb{F}_q[t]$ (Pollack, Sawin/Shusterman):
  - Current: infinitely many $P, P+K$ irreducible pairs for $q > 685090p^2$
  - Geometric methods + stronger analytic results $\rightarrow$ avoid sieves altogether
  - Better distribution results exceed Bombieri-Vinogradov
  - In principle, seems like parity is not an issue, but usually better methods than sieves

Conclusion

Conclusion

- Sieves are simple tools that can achieve surprising results on their own
- Their simplicity leaves them open to the parity problem
- How to beat parity varies depending on setting, and relies on injecting available analytic information