Sieve methods in number theory

Noha Nasri

Euler Circle IRPW

July 11, 2025

Sieve Methods

Sieve methods are advanced techniques in number theory used to count the number of elements with certain properties within larger sets of numbers. The first sieve, developed by Eratosthenes in the third century BC, is intuitive and works like a prime counting algorithm.
In the 20th century, Viggo Brun developed Brun's sieve and applied it to deduce interesting results, such as the convergence of the sum of reciprocals of twin primes. Over the years, mathematicians developed other sieve methods: Selberg's sieve, Turán's sieve, Rosser's sieve, the large sieve, and more.

The Sieve of Eratosthenes

The sieve works by starting with a list of integers $2, 3, \ldots, x$.
- First, call 2 prime and cross out all multiples of 2. - Then, call 3 prime and cross out all multiples of 3. - Continue by picking the next uncrossed number and repeat.
The process stops once we reach the next uncrossed integer m such that $m \geq \sqrt{x}$. All remaining uncrossed numbers are prime.

Big O Notation

Let $D \subseteq \mathbb{C}$ and $f : D \to \mathbb{C}$. We write

$$f(x) = O(g(x))$$

if there exists a positive constant A such that

$$|f(x)| \leq Ag(x) \quad \text{for all } x \in D,$$

where $g : D \to \mathbb{R}^+$. Typically, D is $\mathbb{N}$ or $\mathbb{R}_0^+$.
Sometimes, the notation

$$f(x) \ll g(x) \quad \text{or} \quad g(x) \gg f(x)$$

is used to mean $f(x) = O(g(x))$.

The Möbius Function

The **Möbius function** $\mu(\cdot)$ is multiplicative and defined by:

$$\mu(1) = 1, \quad \mu(p) = -1 \text{ for every prime } p, \quad \mu(p^a) = 0 \text{ for } a \geq 2.$$

Thus: - $\mu(n) = 0$ if n is not squarefree, - $\mu(n) = (-1)^k$ if n is the product of k distinct primes.

Lemma (Fundamental Property)

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Starting Point: Definition of $\Phi(x, z)$

Let

$$P(z) = \prod_{p<z} p,$$

the product of all primes less than z.
The sieve of Eratosthenes removes all numbers not coprime to $P(z)$ (except primes dividing $P(z)$ themselves). This motivates the study of the function

$$\Phi(x, z) = \#\{n \leq x : n \text{ is not divisible by any prime } p < z\}.$$

Theorem

Theorem

$$\Phi(x,z) = x\prod_{p<z}\left(1-\frac{1}{p}\right) + O(2^z).$$

Proof (Part 1)

$$\phi(x,z) = \sum_{\substack{n \leq x \\ \gcd(n,P(z))=1}} 1$$

Using lemma the fundamental property of the Möbius function:

$$\phi(x,z) = \sum_{n \leq x} \left(\sum_{d \mid \gcd(n,P(z))} \mu(d) \right) = \sum_{n \leq x} \left(\sum_{\substack{d \mid n \\ d \mid P(z)}} \mu(d) \right)$$

We rearrange the sum, by putting the sum over d dividing $P(z)$ on the outside, and for each of these divisors, we sum over all n less than or equal to x that are divisible by d.

$$\Phi(x,z) = \sum_{d|P(z)} \mu(d) \left(\sum_{\substack{n \leq x \\ d|n}} 1 \right) = \sum_{d|P(z)} \mu(d) \left(\sum_{m \leq \frac{x}{d}} 1 \right)$$

The last step follows by substituting $n = m \cdot d$, so that the sum over all positive integers $n \leq x$ such that n is a multiple of d becomes the sum over all positive integers $m \leq \frac{x}{d}$.

$$\sum_{m \leq \frac{x}{d}} 1 = \left\lfloor \frac{x}{d} \right\rfloor = \frac{x}{d} + O(1)$$

Proof (Part 2)

Then using the fact that $|\mu(d)| \leq 1$ for all d,

$$\begin{aligned}\phi(x,z) &= \sum_{d|P(z)} \mu(d) \left\lfloor \frac{x}{d} \right\rfloor \\ &= x \sum_{d|P(z)} \frac{\mu(d)}{d} + O\left(\sum_{d|P(z)} 1 \right)\end{aligned}$$

The sum in the error term is to count the number of subsets of the set of primes less than or equal to z, which bounded by 2^z.

For the main term:

$$x \sum_{d|P(z)} \frac{\mu(d)}{d} = x \left(1 + \sum_{p|P(z)} \frac{\mu(p)}{p} + \sum_{p_1<p_2|P(z)} \frac{\mu(p_1 p_2)}{p_1 p_2} + \cdots \right)$$

$$= x \left(1 - \sum_{p|P(z)} \frac{1}{p} + \sum_{p_1<p_2|P(z)} \frac{1}{p_1 p_2} - \cdots \right)$$

Observe that in this sum, we either choose a 1 or a $\frac{-1}{p}$, so:

$$x \sum_{d|P(z)} \frac{\mu(d)}{d} = x \prod_{p \leq z} \left(1 - \frac{1}{p} \right)$$

Thus:

$$\phi(x, z) = x \prod_{p<z} \left(1 - \frac{1}{p} \right) + O(2^z)$$

Error term improvement

We want to refine the error term obtained in the previous subsection, Let's introduce the function $\psi(x, z)$:

$$\psi(x, z) = \#\{n \leq x : p \mid n \Rightarrow p \leq z\}$$

Recall that:

$$\phi(x, z) = \sum_{d \mid P(z)} \mu(d) \left\lfloor \frac{x}{d} \right\rfloor$$

Note that the term $\left\lfloor \frac{x}{d} \right\rfloor$ is only nonzero when $d \leq x$. This implies that we are only summing over divisors of $P(z)$ that are less than or equal to x. Hence:

$$\phi(x,z) = x \sum_{\substack{d \leq x \\ d \mid P(z)}} \frac{\mu(d)}{d} + O\left(\psi(x,z)\right)$$

we will use Rankin's trick to show that:

$$\psi(x,z) \ll x(\log z) \exp\left(-\frac{\log x}{\log z}\right)$$

Main term

$$\sum_{\substack{d|P(z)\\ d\leq Z}} \frac{\mu(d)}{d} = \prod_{p<z}\left(1-\frac{1}{p}\right) + O\left(x(\log x)^2 \exp\left(-\frac{\log x}{\log z}\right)\right).$$

Final approximation

$$\Phi(x,z) = x\prod_{p<z}\left(1-\frac{1}{p}\right) + O\left(x(\log z)^2 \exp\left(-\frac{\log x}{\log z}\right)\right), \quad \text{as } x, z \to \infty.$$

The Generalized Sieve of Eratosthenes

Let $\mathcal{A}$ be any set of natural numbers $\leq x$ and let $\mathcal{P}$ be a set of primes. To each prime $p \in \mathcal{P}$, associate $\omega(p)$ distinguished residue classes modulo p. Let $\mathcal{A}_p$ denote the subset of elements in $\mathcal{A}$ that belong to at least one of the residue classes modulo p. Set $\mathcal{A}_1 := \mathcal{A}$, and for any squarefree integer d composed only of primes from $\mathcal{P}$, define:

$$\mathcal{A}_d := \bigcap_{p|d} \mathcal{A}_p$$

and

$$\omega(d) := \prod_{p|d} \omega(p).$$

Let z be a positive real number and define:

$$P(z) := \prod_{\substack{p \in \mathcal{P} \\ p<z}} p.$$

The Generalized Sieve of Eratosthenes

We denote by $S(\mathcal{A}, \mathcal{P}, z)$ the number of elements of the sifted set:

$$\mathcal{A} \setminus \bigcup_{p|P(z)} \mathcal{A}_p.$$

We assume that there exists a constant X such that for every squarefree d composed of primes from $\mathcal{P}$, the cardinality of $\mathcal{A}_d$ satisfies:

$$\#\mathcal{A}_d = \frac{\omega(d)}{d} X + R_d \tag{5.3}$$

for some remainder term R_d.

Theorem: Generalized Sieve of Eratosthenes

Suppose:

1. $|R_d| = O(\omega(d))$;
2. $\displaystyle\sum_{p|P(z)} \frac{\omega(p)\log p}{p} \leq \kappa \log z + O(1)$ for some $\kappa \geq 0$;
3. $\#\mathcal{A}_d = 0$ for all $d > y > 0$.

Then

$$S(\mathcal{A}, \mathcal{P}, z) = XW(z) + O\left(\left(X + \frac{y}{\log z}\right)(\log z)^{\kappa+1} \exp\left(-\frac{\log y}{\log z}\right)\right),$$

where

$$W(z) = \prod_{\substack{p \in \mathcal{P} \\ p < z}} \left(1 - \frac{\omega(p)}{p}\right).$$

THANK YOU!