Sieve Methods

Bailey Whitbread

University of Queensland

August 21, 2020

A Classic Sieve

Sieve of Eratosthenes

Introduction to Arithmetic, Nicomachus (60-120 AD).

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120

Given

1. a finite integer set $\mathcal{A} \subset \mathbb{Z}$,
2. a set of primes $\mathcal{P}$,
3. an integer $z > 1$.

We remove elements from $\mathcal{A}$ that are divisible by primes $p \in \mathcal{P}$ with $p \leq z$.

This is called *sifting* $\mathcal{A}$ by $\mathcal{P}$.

Define

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

then we say $\mathcal{P}$ *sifts out* $n \in \mathcal{A}$ if $\gcd(n, P(z)) > 1$.

The leftover after $\mathcal{A}$ is sifted by $\mathcal{P}$ is the set

$$S(\mathcal{A}, \mathcal{P}, z) = |\{a \in \mathcal{A} : (a, P(z)) = 1\}|$$

Sieve Formulation

Sieve of Eratosthene's: $\mathcal{A} = \{1, 2, 3, ..., N\}$, $\mathcal{P} = \{\text{all primes}\}$ and $z = [N^{1/2} + 1]$. Then we observe

$$S(\mathcal{A}, \mathcal{P}, z) = \sum_{\substack{a \in \mathcal{A} \\ (a, P(z))=1}} 1$$

$$= 1 + \sum_{\substack{1 < n \leq N^{1/2} \\ (n, P(z))=1}} 1 + \sum_{\substack{N^{1/2} < n \leq N \\ (n, P(z))=1}} 1$$

$$= 1 + \pi(N) - \pi(N^{1/2}).$$

A Weak Prime Number Theorem

Recall the Mobius function

$$\mu(m) = \begin{cases} 0, & \text{if } m \text{ not square-free,} \\ 1, & \text{if } m \text{ square-free with even number of prime factors,} \\ -1, & \text{if } m \text{ square-free with odd number of prime factors.} \end{cases}$$

Lemma

If $f : [1, \infty) \to \mathbb{R}$ is multiplicative and $f(1) = 1$ then

$$\sum_{d|n} \mu(d) f(d) = \prod_{p|n} (1 - f(p)).$$

With $\mathcal{A} = \{1, 2, 3, ..., N\}$, $\mathcal{P} = \{\text{all primes}\}$,

$$\begin{aligned} S(\mathcal{A}, \mathcal{P}, z) &= \sum_{\substack{a \in \mathcal{A} \\ (a, P(z)) = 1}} 1 \\ &= \sum_{a \in \mathcal{A}} \sum_{d | (a, P(z))} \mu(d) \\ &= \sum_{a \in \mathcal{A}} \sum_{\substack{d | a \\ d | P(z)}} \mu(d) \\ &= \sum_{d | P(z)} \mu(d) \left[\sum_{\substack{a \in \mathcal{A} \\ d | a}} 1 \right] \\ &= \sum_{d | P(z)} \mu(d) |\mathcal{A}_d|, \text{ where } \mathcal{A}_d = \{a \in \mathcal{A} : d | a\}. \end{aligned}$$

A Weak Prime Number Theorem

In our case, $|\mathcal{A}_d| = [N/d] = N/d - \{N/d\}$. Then

$$\begin{aligned} S(\mathcal{A}, \mathcal{P}, z) &= \sum_{d|P(z)} \mu(d)|\mathcal{A}_d| \\ &= \sum_{d|P(z)} \mu(d)(N/d - \{N/d\}) \\ &= N \sum_{d|P(z)} \frac{\mu(d)}{d} - \sum_{d|P(z)} \mu(d)\{N/d\}. \end{aligned}$$

Our lemma with $f(x) = 1/x$ tells us

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

A Weak Prime Number Theorem

Then

$$S(\mathcal{A}, \mathcal{P}, z) = N \prod_{p | P(z)} \left(1 - \frac{1}{p}\right) + R,$$

with

$$R = - \sum_{d | P(z)} \mu(d) \{N/d\} = \sum_{d | P(z)} \mathcal{O}(1) = \mathcal{O}(2^{\pi(z)}).$$

Set $z = \log N$, then

$$2^{\pi(z)} = 2^{\pi(\log N)} \leq 2^{\log N} = e^{\log N \ \log 2} = N^{\log 2}.$$

Then $R = \mathcal{O}(2^{\pi(z)}) = \mathcal{O}(N^{\log 2})$.

A Weak Prime Number Theorem

Notice

$$S(\mathcal{A},\mathcal{P},z) \geq 1 + \pi(N) - \pi(z) \geq \pi(N) - z.$$

Then

$$\begin{aligned}
\pi(N) &\leq z + S(\mathcal{A},\mathcal{P},z) \\
&= \log N + N \prod_{p|P(z)} \left(1 - \frac{1}{p}\right) + \mathcal{O}(N^{\log 2}) \\
&= N \prod_{p|P(z)} \left(1 - \frac{1}{p}\right) + \mathcal{O}(N^{\log 2}).
\end{aligned}$$

A Weak Prime Number Theorem

Lastly,

$$\begin{aligned}
\prod_{p \mid P(z)} \left(1 - \frac{1}{p}\right)^{-1} &= \prod_{p<z} \left(1 - \frac{1}{p}\right)^{-1} \\
&= \prod_{p<z} \sum_{m \geq 0} \frac{1}{p^m} \\
&> \sum_{n<z} \frac{1}{n} \\
&> \int_1^z \frac{1}{x} \, \mathrm{d}x \\
&= \log z.
\end{aligned}$$

A Weak Prime Number Theorem

Finally,

$$\prod_{p|P(z)} \left(1 - \frac{1}{p}\right) < \frac{1}{\log z} = \frac{1}{\log\log N}.$$

Thus

$$\pi(N) = N \prod_{p|P(z)} \left(1 - \frac{1}{p}\right) + \mathcal{O}(N^{\log 2}) < \frac{N}{\log\log N} + \mathcal{O}(N^{\log 2}).$$