CTNT 2020: Introduction to Sieves

Brandon Alberts

University of Connecticut

June 2020

Introduction

Definition

A **sieve** is a tool for separating desired objects from other objects.

Examples:

- A pasta strainer separates pasta from water.
- Sieves were used during the gold rush to separate gold from sand and dirt.
- The Sieve of Eratosthenes separates primes numbers from all other numbers.

Sieve of Eratosthenes

1	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

If $n \le x$ is not prime, then $n = p \cdot a$ where p is a prime $p \le \sqrt{x}$

Asymptotic Notation and Arithmetic Functions

Definition

An **arithmetic function** is a function $f : \mathbb{N} \to \mathbb{C}$. These functions can be used to capture and study certain arithmetic behaviors.

$\boxed{\text{Ex}}$

- $\nu(n) = \#\{\text{distinct prime divisors } p \mid n\}$
  (or $\omega(n)$)
- $d(n) = \#\{\text{divisors } d \mid n\}$
  (or $\sigma_0(n)$)
- $\varphi(n) = \#\{1 \leq d < n : \gcd(d, n) = 1\}$
  (or $\phi(n)$) $\qquad |(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$
- If $A \subseteq \mathbb{N}$

$$1_A(n) = \begin{cases} 1 & n \in A \\ 0 & n \notin A \end{cases}$$

Arithmetic functions often have very erratic behavior, which makes them more difficult to deal with using analytic techniques. Consider the divisor function $d(n) = \#\{\text{positive divisors of } n\}$. (see CoCalc)

If $n =$ prime, then

$$d(n) = 2$$

If $n = 2^k$, then

$$d(2^k) = k+1$$

We can smooth out the information contained in an arithmetic function by considering the function of a real variable x

$$\sum_{n \leqslant x} d(n)$$

$\sum_{n\leq x} d(n)$ is "close to" $x\log x$

"$\log x$" $= \ln x$ or log base e

Definition

Let $f(x)$ and $g(x)$ be two functions and let $x \to \infty$. We say $f(x)$ is **asymptotic to** $g(x)$ and write $f(x) \sim g(x)$ if

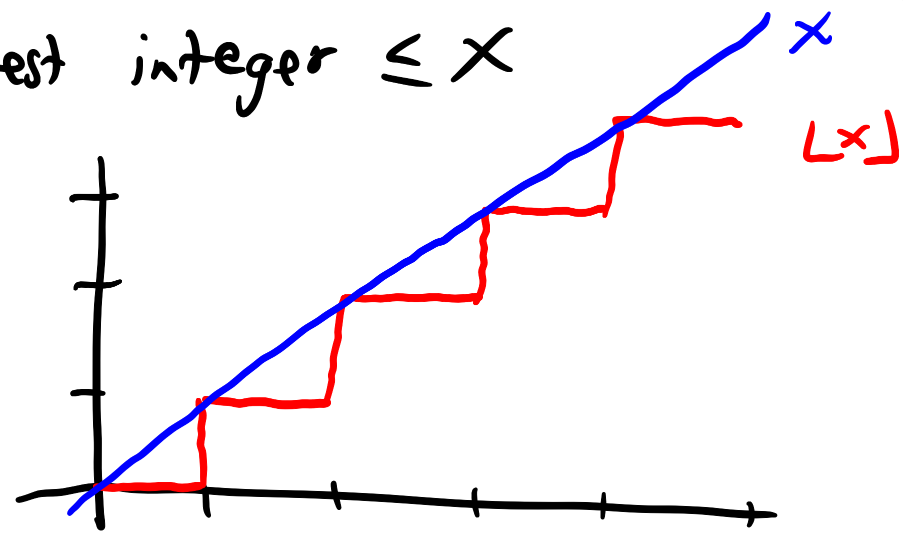
$$\lim_{x \to \infty} \frac{f(x)}{g(x)} = 1 .$$

CoCalc suggests that $\sum_{n \leq x} d(n) \sim x \log x$

or $\lim_{x \to \infty} \frac{\sum_{n \leq x} d(n)}{x \log x} = 1$

Ex) floor function $\lfloor x \rfloor :=$ greatest integer $\leq x$

alternatively $\lfloor x \rfloor = \sum_{n \leq x} 1$



Lemma

$\lfloor x \rfloor \sim x$

Pf We know $\lfloor x \rfloor \leq x$ by def.

Also, $\lfloor x \rfloor + 1 > x \Rightarrow \lfloor x \rfloor > x - 1$

We want to find $\lim_{x \to \infty} \frac{\lfloor x \rfloor}{x}$

$$1 - \frac{1}{x} = \frac{x-1}{x} < \frac{\lfloor x \rfloor}{x} \leq \frac{x}{x} = 1$$

$\lim_{x \to \infty} 1 - \frac{1}{x} = 1$ $\qquad \lim_{x \to \infty} 1 = 1$

So the Squeeze Thm implies

$$\lim_{x \to \infty} \frac{\lfloor x \rfloor}{x} = 1 \qquad \square$$

Definition

Let $f(x)$ and $g(x)$ be function of the real variable x. We define the following:

(a) $f(x)$ is **little-oh** of $g(x)$, written $\boxed{f(x) = o(g(x))}$, if

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0\,.$$

In this case, $f(x)$ is "asymptotically smaller" than $g(x)$.

(b) $f(x)$ is **big-oh** of $g(x)$, written $\boxed{f(x) = O(g(x))}$ or $\boxed{f(x) \ll g(x)}$, if there exists a constant $C > 0$ such that $\boxed{|f(x)| \leqslant C \cdot |g(x)|}$ for all $x \geqslant x_0$. Equivalently,

$$\limsup_{x\to\infty} \frac{f(x)}{g(x)} < \infty\,.$$

In this case, $f(x)$ is "asymptotically the same order of magnitude or smaller" than $g(x)$.

Exercise: If $f(x) \sim g(x)$ then $f(x) = O(g(x))$.

Definition

We write

$$f(x) = \underbrace{g(x)}_{\text{main term}} + \underbrace{O(h(x))}_{\text{error term}}$$

to mean

$$f(x) - g(x) = O(h(x)).$$

Similar notation applies to little-oh.

Exercise: $O(h(x))$ and $o(h(x))$ are ideals in the ring of functions defined for x sufficiently large. The above notation is then equivalent to stating that $f(x)$ and $g(x)$ belong to the same coset when quotienting by the ideal $O(h(x))$.

Lemma

$$\lfloor x \rfloor = \underbrace{x}_{\text{main term}} + \underbrace{O(1)}_{\text{error term}}$$

Pf We want bound $|\lfloor x \rfloor - x|$

We know $\lfloor x \rfloor \le x$ and $\lfloor x \rfloor > x-1$

$$\Rightarrow \quad -1 < \lfloor x \rfloor - x \le 0$$

$$\Rightarrow \quad |\lfloor x \rfloor - x| \le 1$$

So there exists a constant $C>0$ s.t. $(C=1)$

$$|\lfloor x \rfloor - x| \le C \cdot 1 \text{ for all } x \geq 0$$

$$\Rightarrow \lfloor x \rfloor - x = O(1)$$

$\square$

Exercises:

1. $f(x) \cdot O(g(x)) = O(f(x)g(x))$ and $f(x) \cdot o(g(x)) = o(f(x) \cdot g(x))$,
   If $h(x) = O(g(x))$ then $f(x)h(x) = O(f(x)g(x))$
2. If $f(x) = O(g(x))$ and $h(x) = O(g(x))$ then $f(x) + h(x) = O(g(x))$,
3. If $f(x) = O(g(x))$ and $g(x) = O(h(x))$, then $f(x) = O(h(x))$.
4. If $f(x) = O(g(x))$, then $\sum_{n \leqslant x} f(n) = O\left(\sum_{n \leqslant x} g(n)\right)$.
5. If $f(x) = O(g(x))$ and y is some real number, then $\int_y^x f(t)dt = O\left(\int_y^x g(t)dt\right)$.

Abel Summation

Abel Summation

Theorem

Write $A(x) = \sum_{n \leqslant x} a_n$ and suppose $f(t)$ is a differentiable function on the interval (y, x) for $y < x < \infty$. Then

$$\sum_{y < n \leqslant x} a_n f(n) = A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t)dt\,.$$

$A(t)$ is like a "discrete antiderivative" of a_n, and we can recognize the familar integration by parts formula with $u = f(t)$ and "dv" $= a_n$:

$$\sum_{y < n \leqslant x} a_n f(n) = A(t)f(t)\Big|_y^x - \int_y^x A(t)f'(t)dt$$

$u = f(t)$ $\qquad$ $du = f'(t)\,dt$

"dv" $= a_n$ $\qquad$ "v" $= \sum_{n \leq t} a_n = A(t)$

Corollary

$$\sum_{n\leqslant x}\frac{1}{n}=\boxed{\log x}+\boxed{O(1)}$$

Abel Summation $\quad a_n=1 \quad f(t)=\frac{1}{t}$

$A(t)=\lfloor t\rfloor \quad f'(t)=-\frac{1}{t^2}$

$$\frac{1}{1}+\sum_{1<n\leq x}\frac{1}{n}=\frac{1}{1}+\lfloor t\rfloor\cdot\frac{1}{t}\Big|_1^x-\int_1^x\lfloor t\rfloor\left(-\frac{1}{t^2}\right)dt$$

$$=\frac{\lfloor x\rfloor}{x}+\int_1^x\frac{\lfloor t\rfloor}{t^2}\,dt$$

$\lfloor t\rfloor=t+O(1)$

$$=\frac{x+O(1)}{x}+\int_1^x\frac{t+O(1)}{t^2}\,dt$$

$O\left(1-\frac{1}{x}\right)$

$$=\boxed{1}+\boxed{O\left(\frac{1}{x}\right)}+\boxed{\int_1^x\frac{1}{t}\,dt}+\boxed{O\left(\int_1^x\frac{1}{t^2}\,dt\right)}$$

Theorem

$$\sum_{n \leq x} d(n) = x \log x + O(x)$$

Pf $\quad d(n) = \#\{\text{positive } d \mid n\} = \sum_{d \mid n} 1 = \sum_{da = n} 1$

$d \mid n$ means $n = d \cdot a$ for some positive int. a

$$\sum_{n \leq x} d(n) = \sum_{n \leq x} \sum_{da = n} 1 = \sum_{da \leq x} 1$$

$$= \sum_{d \leq x} \left(\sum_{a \leq \frac{x}{d}} 1 \right)$$

$$= \sum_{d \leq x} \left\lfloor \frac{x}{d} \right\rfloor$$

$$\sum_{n\le x} d(n) = \sum_{d\le x} \left\lfloor \frac{x}{d} \right\rfloor$$

$$= \sum_{d\le x} \left(\frac{x}{d} + O(1) \right)$$

$$= x\left(\sum_{d\le x} \frac{1}{d}\right) + O\left(\sum_{d\le x} 1\right)$$

$$= x\left(\log x + O(1)\right) + O(\lfloor x \rfloor)$$

$$= x \log x + O(x) + O(\lfloor x \rfloor)$$

$\lfloor x \rfloor \le x$, so $\lfloor x \rfloor = O(x)$

$\square$

Möbius function

Definition

The **Möbius function** is defined as follows:

$\mu(1)=1$ $\mu(3)=-1$
$\mu(2)=-1$ $\mu(4)=0$ ...
etc

$$\mu(n) = \begin{cases} (-1)^k & n = \prod_{i=1}^{k} p_i \text{ is a product of } k \text{ distinct primes} \\ 0 & \text{otherwise} \end{cases}$$

Lemma

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & n = 1 \\ 0 & n \neq 1 \end{cases}$$

Pf $\underline{n=1}$ $\quad \sum_{d|1} \mu(d) = \mu(1) = 1$

$\underline{n = \prod_{i=1}^{k} p_i^{e_{p_i}}}$

$$\sum_{d|n} \mu(d) = \mu(1) + \sum_{i=1}^{k} \mu(p_i) + \sum_{\{i,j\}} \mu(p_i p_j) + \dots + \mu(p_1 \cdots p_k)$$

$$= \binom{k}{0} + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + \dots + \binom{k}{k}(-1)^k$$

Binomial Theorem

$$= ((-1)+1)^k = 0$$

$\square$

Theorem (Mobius Inversion)

If $\boxed{f(n) = \sum_{d|n} g(d)}$ *then* $g(n) = \sum_{d|n} \mu(d) f(n/d)$.

Ex) $\sigma_0(n) = \sum_{d|n} 1 \implies 1 = \sum_{d|n} \mu(d)\, \sigma_0\left(\frac{n}{d}\right)$

Pf)
$$\sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) = \sum_{da=n} \mu(d) \boxed{f(a)}$$
$$= \sum_{da=n} \mu(d) \boxed{\left(\sum_{b|a} g(b)\right)}$$
$$= \sum_{da=n} \mu(d) \left(\sum_{bc=a} g(b)\right)$$
$$= \sum_{dbc=n} \mu(d)\, g(b)$$
$$= \sum_{b|n} g(b) \left(\sum_{d \cdot c = \frac{n}{b}} \mu(d)\right)$$

$$\sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) = \sum_{b|n} g(b) \left(\sum_{dc = \frac{n}{b}} \mu(d) \right)$$

$$= \sum_{b|n} g(b) \underbrace{\left(\sum_{d | \frac{n}{b}} \mu(d) \right)}_{\begin{cases} 1 & \text{if } \frac{n}{b} = 1 \quad \text{i.e. } b = n \\ 0 & \text{if } \frac{n}{b} \neq 1 \quad \text{i.e. } b \neq n \end{cases}}$$

$$= 0 + 0 + \cdots + g(n) \cdot 1$$

$\square$

Squarefree numbers

inclusion-exclusion

$$\lfloor x \rfloor$$

$$-\left\lfloor \frac{x}{2^2} \right\rfloor - \left\lfloor \frac{x}{3^2} \right\rfloor - \left\lfloor \frac{x}{5^2} \right\rfloor - \left\lfloor \frac{x}{7^2} \right\rfloor - \cdots$$

$$+\left\lfloor \frac{x}{2^2 \cdot 3^2} \right\rfloor + \left\lfloor \frac{x}{2^2 \cdot 5^2} \right\rfloor + \left\lfloor \frac{x}{3^2 \cdot 5^2} \right\rfloor + \cdots$$

$$-\left\lfloor \frac{x}{2^2 \cdot 3^2 \cdot 5^2} \right\rfloor - \cdots$$

+ etc...

$$= \sum_d \mu(d) \left\lfloor \frac{x}{d^2} \right\rfloor$$

1	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

Theorem

$$\#\{\text{squarefree numbers } \leqslant x\} = \left(\sum_{n=1}^{\infty} \frac{\mu(n)}{n^2}\right) x + O(\sqrt{x})$$

$$\frac{6}{\pi^2} x + O(\sqrt{x})$$

Pf) $\sum_{d} \mu(d) \left\lfloor \frac{x}{d^2} \right\rfloor$

$\left\lfloor \frac{x}{d^2} \right\rfloor = 0$ if $d^2 > x$

i.e. $d > \sqrt{x}$

$$= \sum_{d \leq \sqrt{x}} \mu(d) \left\lfloor \frac{x}{d^2} \right\rfloor$$

$$= \sum_{d \leq \sqrt{x}} \mu(d) \left(\frac{x}{d^2} + O(1) \right)$$

$$= \left(\sum_{d \leq \sqrt{x}} \frac{\mu(d)}{d^2} \right) x + \underbrace{O\left(\sum_{d \leq \sqrt{x}} 1 \right)}_{O(\lfloor \sqrt{x} \rfloor)}$$

$$\left(\sum_{d\le\sqrt{x}} \frac{\mu(d)}{d^2}\right)x = \left(\sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} - \sum_{\sqrt{x}<d} \frac{\mu(d)}{d^2}\right)x$$

only makes sense if $\sum_{d=1}^{\infty} \frac{\mu(d)}{d^2}$ converges

$$\left|\frac{\mu(d)}{d^2}\right| \le \left|\frac{1}{d^2}\right|$$

so converges by comparison with $\sum_{d=1}^{\infty} \frac{1}{d^2}$

$$= \left(\sum_{d=1}^{\infty} \frac{\mu(d)}{d^2}\right)x - \left(\sum_{\sqrt{x}<d} \frac{\mu(d)}{d^2}\right)x$$

$a_n = 1 \qquad f(t) = \frac{1}{t^2}$

$A(t) = \lfloor t \rfloor \qquad f'(t) = \frac{-2}{t^3}dt$

$$\left|\sum_{\sqrt{x}<d} \frac{\mu(d)}{d^2}\right| \le \left|\sum_{\sqrt{x}<d\le\infty} \frac{1}{d^2}\right|$$

$$\le \left|\frac{\lfloor t \rfloor}{t^2}\Big|_{\sqrt{x}}^{\infty}\right| + \left|2\int_{\sqrt{x}}^{\infty} \frac{\lfloor t \rfloor}{t^3}\,dt\right|$$

$\cancel{\lfloor t \rfloor = t + O(1)}$

$\lfloor t \rfloor \le t$

$$\le \left|\frac{1}{t}\Big|_{\sqrt{x}}^{\infty}\right| + \left|2\int_{\sqrt{x}}^{\infty} \frac{1}{t^2}\,dt\right| \ll \frac{1}{\sqrt{x}}$$

Prime Numbers

Theorem (Prime Number Theorem)

Let $\pi(x) = \#\{\text{primes } p \leqslant x\} = \sum_{p \leqslant x} 1$. *Then*

$$\pi(x) \sim \frac{x}{\log x}$$

There are variety of proofs of the PNT, the most accessible of which require complex analytic techniques. There does exist an "elementary proof" (i.e. one that does not appeal to complex analysis), but it is too long to treat in this course.

Theorem (Chebysheff's Theorem)

$$\pi(x) = O\left(\frac{x}{\log x}\right)$$

Exercise: $\pi(x) = O\left(\frac{x}{\log x}\right)$ if and only if $\theta(x) := \sum_{p\leqslant x} \log p = O(x)$.

Pf] Observe that

$$\prod_{n<p\leq 2n} p \,\Big|\, \binom{2n}{n} = \frac{(2n)!}{n!\,n!} \leq 2^{2n}$$

$$2^{2n} = (1+1)^{2n} = \sum_{i=0}^{2n} \binom{2n}{i} \cdot (1)^i$$

$$\sum_{n<p\leq 2n} \log p \leq 2n \log 2$$

$$\theta(2n) - \theta(n) \leq 2n \log 2$$

$\star$ $\theta(2n) - \theta(n) \leq 2n \log 2$

We will prove $\theta(n) \leq 4n \log 2$

<u>base case</u> $n=1$, $\theta(1) = \sum_{p \leq 1} \log p = 0 \leq 4 \cdot 1 \cdot \log 2$ ✓

<u>inductive step</u> suppose for all $1 \leq k < n$, $\theta(k) \leq 4k \log 2$

<u>n = even</u> $\star$ $\theta(n) - \theta\left(\frac{n}{2}\right) \leq n \log 2$

$$\theta(n) \leq n \log 2 + \theta\left(\frac{n}{2}\right)$$

$$\leq n \log 2 + 4\left(\frac{n}{2}\right) \log 2 \qquad \text{I.H.}$$

$$\leq 3n \log 2 \leq 4n \log 2$$

<u>n = odd ≥ 3</u> $n+1$ is even and $\geq 4 \Rightarrow n+1$ is <u>not prime</u>

$$\theta(n) = \sum_{p \leq n} \log p = \sum_{p \leq n+1} \log p = \theta(n+1)$$

$n+1$ is even and $\frac{n+1}{2} < n$

$\star$ $\theta(n) = \theta(n+1) \leq (n+1) \log 2 + \theta\left(\frac{n+1}{2}\right)$

$$\Theta(n) \le (n+1)\log 2 + \Theta\left(\frac{n+1}{2}\right)$$

$$\le (n+1)\log 2 + 4\left(\frac{n+1}{2}\right)\log 2 \qquad \text{I.H.}$$

$$\le 3(n+1)\log 2$$

$$\le 4n\log 2 \quad \text{by } n \geq 3 \qquad \square$$

$$\Rightarrow \Theta(n) = O(n)$$

Theorem

$$\sum_{p\leqslant x} \frac{\log p}{p} = \log x + O(1)$$

Exercise $\displaystyle\sum_{n\leq x} \log(n) = x\log x - x + O(\log x)$

Pf] $\displaystyle n! = \prod_p p^{e_p} = \prod_{k=1}^{n} k$

$$e_p = \underbrace{\left\lfloor \frac{n}{p} \right\rfloor}_{\substack{\#\, d\leq n \\ \text{s.t. } p\mid d}} + \underbrace{\left\lfloor \frac{n}{p^2} \right\rfloor}_{\substack{\#\, d\leq n \\ \text{s.t. } p^2\mid d}} + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots$$

$$\sum_{p\leq n} e_p \log p = \sum_{k\leq n} \log k = n\log n - n + O(\log n)$$

$$\sum_{p \le n} \log p \left(\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots \right) = n \log n - n + O(\log n)$$

leading term

$$\sum_{p \le n} \log p \left\lfloor \frac{n}{p} \right\rfloor = \sum_{p \le n} \log p \left(\frac{n}{p} + O(1) \right)$$

$$= n \sum_{p \le n} \frac{\log p}{p} + O\left(\sum_{p \le n} \log p \right)$$

$$= n \sum_{p \le n} \frac{\log p}{p} + O(n)$$

chebyshoff's thm

everything else

$$\sum_{p \le n} \log p \left(\left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots \right) \le \sum_{p \le n} \log p \cdot \sum_{i=2}^{\infty} \frac{n}{p^i}$$

$$= \sum_{p \le n} \log p \cdot \left(\frac{n/p^2}{1 - 1/p} \right)$$

$$= n \boxed{\sum_{p \le n} \frac{\log p}{p(p-1)}}$$

converges as $n \to \infty$

$\le \sum \frac{1}{n^{3/2}}$

$$= O(n)$$

$$n\sum_{p\le n}\frac{\log p}{p} + O(n) + O(n) = n\log n - n + O(\log n)$$

$$\sum_{p\le n}\frac{\log p}{p} + \underbrace{O(1)} + \underbrace{O(1)} = \log n \underbrace{-1} + \underbrace{O\left(\frac{\log n}{n}\right)}$$

these are $O(1)$

$\square$

Corollary

$$\sum_{p \leqslant x} \frac{1}{p} = \log \log x + O(1)$$

Exercise: Prove this corollary using Abel Summation with $f(t) = (\log t)^{-1}$.

Corollary $\sum_p \frac{1}{p}$ diverges by taking $x \to \infty$

Sieve of Eratosthenes

Eratosthenes sieved out numbers divisible by small primes. We can this by considering the function

$$\Phi(x,z) = \#\{n \leqslant x : n \text{ is not divisible by any primes } < z\}$$

intermediate step of the sieve

where x and z are positive real numbers.

Theorem

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

certainly ≤ 1

as $z \to \infty$, prod $\to 0$

grows very fast in z

if z is too big, $O(2^z)$ will be bigger than the "main term"

ex) $z = \log\log x$

$O(2^{\log\log x}) = O(\log x)$

$x \prod_{p<\log\log x}\left(1-\frac{1}{p}\right)$ grows like what?

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

$\boxed{P(z) = \prod_{p<z} p}$ $\boxed{(a,b) = \gcd(a,b)}$

$$\phi(x,z) = \sum_{\substack{n \le x \\ (n,P(z))=1}} 1 = \sum_{n \le x} \underbrace{\left(\sum_{d \mid (n,P(z))} \mu(d) \right)}_{= \begin{cases} 1 & \text{if } (n,P(z))=1 \\ 0 & \text{if } (n,P(z)) \ne 1 \end{cases}}$$

$$= \sum_{n \le x} \sum_{\substack{d \mid n \\ d \mid P(z)}} \mu(d)$$

$$= \sum_{d \mid P(z)} \mu(d) \boxed{\left(\sum_{\substack{n \le x \\ d \mid n}} 1 \right)}$$

if $d \mid n$
write $n = m \cdot d$
$n \le x \iff m \le \frac{x}{d}$

$$\boxed{\sum_{m \le \frac{x}{d}} 1} = \left\lfloor \frac{x}{d} \right\rfloor$$

$$\phi(x,z) = \sum_{d \mid P(z)} \mu(d) \left\lfloor \frac{x}{d} \right\rfloor = \sum_{d \mid P(z)} \mu(d) \left(\frac{x}{d} + O(1) \right)$$

nonzero for $d \le x$

$$= x \sum_{\substack{d \mid P(z) \\ d \le x}} \frac{\mu(d)}{d} + O\left(\sum_{\substack{d \mid P(z) \\ d \le x}} 1 \right)$$

$|\mu(d)| \le 1$

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

$P(z) = \prod_{p<z} p$ product of $\le z$ primes

$d \mid P(z) \Rightarrow d = \prod_{\substack{\text{subset} \\ \text{of } p<z}} p$

$$= x \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\left(1 - \frac{1}{p_3}\right) \cdots$$

# of subsets of set of size z $= 2^z$

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

$\square$

To improve on the error $O(2^z)$, consider the function

$$\Psi(x,z) = \#\{n \leqslant x : \underbrace{\text{if } p \mid n \text{ then } p < z}_{n \text{ is a } \underline{z\text{-smooth number}}}\}$$

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

$$= \sum_{\substack{d \leq x \\ d \mid P(z)}} \mu(d) \left(\frac{x}{d} + O(1) \right)$$

$$= x \sum_{\substack{d \leq x \\ d \mid P(z)}} \mu(d) + \underbrace{O\left(\Psi(x,z)\right)}_{\text{① bound this}}$$

② make sure this doesn't break anything

Theorem

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

compare to 2^z

$\#\{n \le x\}$ $= O(x)$

Rankin's trick

$$\Psi(x,z) = \sum_{\substack{n \le x \\ p \mid n \Rightarrow p < z}} 1$$

$$\le \sum_{\substack{n \le x \\ p \mid n \Rightarrow p < z}} \left(\frac{x}{n}\right)^{\delta}$$ for some $\delta > 0$

$$\le x^{\delta} \sum_{\substack{n \\ p \mid n \Rightarrow p < z}} \frac{1}{n^{\delta}}$$

$$= x^{\delta} \prod_{p < z} \left(1 + \frac{1}{p^{\delta}} + \frac{1}{p^{2\delta}} + \frac{1}{p^{3\delta}} + \cdots\right)$$

$$= x^{\delta} \prod_{p < z} \left(1 - \frac{1}{p^{\delta}}\right)^{-1}$$

$$\psi(x,z) \le x^{\delta} \prod_{p<z} \left(1 - \frac{1}{p^{\delta}}\right)^{-1}$$

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

converges as $z \to \infty$ if $\boxed{\delta > \frac{1}{2}}$

$$\ll x^{\delta} \prod_{p<z} \left(1 + \frac{1}{p^{\delta}}\right)$$

$1 + x \le e^{x}$

$$\ll x^{\delta} \prod_{p<z} \exp\left(\frac{1}{p^{\delta}}\right)$$

$$= x^{\delta} \exp\left(\sum_{p<z} \frac{1}{p^{\delta}}\right)$$

set $\delta = 1 - \eta$ for η "small"

$$p^{-\delta} = p^{-1} \boxed{e^{\eta \log p}}$$

$e^{x} \le 1 + x e^{x}$

$$\Psi(x,z) \ll x^{1-\eta}\exp\left(\sum_{p<z} p^{-1}\left(1+\eta\log p\, e^{\eta\log p}\right)\right)$$

$$\downarrow \quad e^{\frac{\log p}{\log z}} \le p^{\frac{1}{\log z}} \le z^{\frac{1}{\log z}} = e$$

$$\eta = \frac{1}{\log z}$$

$$\Psi(x,z) \ll x^{1-\frac{1}{\log z}}\exp\left(\sum_{p<z}\frac{1}{p}\left(1+\frac{\log p}{\log z}\cdot e\right)\right)$$

$$\ll x^1\exp\left(-\frac{\log x}{\log z}\right)\exp\left(\boxed{\sum_{p<z}\frac{1}{p}}+\frac{e}{\log z}\boxed{\sum_{p<z}\frac{\log p}{p}}\right)$$

$$\left(\log\log z+\underbrace{O(1)}_{O(1)}\right)+\underbrace{\cancel{\frac{e}{\log z}\left(\log z\right.}}_{O(1)}\left.+\underbrace{O(1)}_{O(1)}\right)$$

$$\ll \underbrace{x^1\exp\left(\frac{-\log x}{\log z}\right)}_{\ll x^1}\ \underbrace{\exp\left(\log\log z\right)}_{\log z}$$

Theorem

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

$$\phi(x,z) = x\sum_{\substack{d\le x\\ d\mid P(z)}}\frac{\mu(d)}{d} + \underbrace{O(\psi(x,z))}_{\ll x\log z\,\exp\left(-\frac{\log x}{\log z}\right)}$$

$$\sum_{\substack{d\le x\\ d\mid P(z)}}\frac{\mu(d)}{d} = \underbrace{\sum_{d\mid P(z)}\frac{\mu(d)}{d}}_{=\prod_{p<z}\left(1-\frac{1}{p}\right)} - \sum_{\substack{d>x\\ d\mid P(z)}}\frac{\mu(d)}{d}$$

$$a_d = \begin{cases}1 & d\mid P(z)\\ 0 & \text{else}\end{cases}$$

$$A(t) = \sum_{\substack{d\mid P(z)\\ d\le t}} 1 \ll \psi(t,z)$$

$$\left|\sum_{\substack{d>x\\ d\mid P(z)}}\frac{\mu(d)}{d}\right| \le \sum_{\substack{d>x\\ d\mid P(z)}}\frac{1}{d} = \boxed{\frac{\psi(t,z)}{t}\Bigg|_x^\infty + \int_x^\infty\frac{\psi(t,x)}{t^2}\,dt}$$

$$f(t) = \frac{1}{t}$$

$$f'(t) = -\frac{1}{t^2}$$

$\square$

Theorem (Merten's Theorem)

$$\prod_{p<z}\left(1-\frac{1}{p}\right) \sim \frac{e^{-\gamma}}{\log z},$$ *where γ is the Euler-Mascheroni constant.*

$$\prod_{p<z}\left(1-\frac{1}{p}\right) \leq \prod_{p<z} \exp\left(-\frac{1}{p}\right) = \exp\left(-\sum_{p<z}\frac{1}{p}\right)$$

$$= \exp(-\log\log z + O(1))$$

$$= O\left(\frac{1}{\log z}\right)$$

$1+x \leq e^x$

$$\boxed{\log z = \frac{\log x}{A\log\log x}}$$

$$x\prod_{p<z}\left(1-\frac{1}{p}\right) \ll \boxed{\frac{A\,x\log\log x}{\log x}}$$

$\log((\log x)^{-A})$

$$O\left(x(\log z)^2\exp\left(-\frac{\log x}{\log z}\right)\right) \ll x\left(\frac{\log x}{A\log\log x}\right)^2 \exp(-A\log\log x)$$

$$\ll \boxed{\frac{x}{A(\log x)^{A-2}(\log\log x)^2}}$$

Let $\mathcal{A}$ be a set of integers $\leqslant x$, $\mathcal{P}$ a set of primes, and $P(z) = \prod_{\substack{p \in \mathcal{P} \\ p < z}} p$.

- For each prime $p \in \mathcal{P}$, let $\mathcal{A}_p \subset \mathcal{A}$ be a subset of integers belonging to $\omega(p)$ distinct residue classes modulo p.

- Define $S(\mathcal{A}, \mathcal{P}, z) = \# \left(\mathcal{A} \backslash \bigcup_{p | P(z)} \mathcal{A}_p \right)$.

Ex) $\mathcal{A} = \{ n \leq x \}$

$\mathcal{A}_p = \{ n \leq x : p | n \}$

- If d is a squarefree number divisible by primes of $\mathcal{P}$, define $\omega(d) = \prod_{p|d} \omega(p)$ and $\mathcal{A}_d = \bigcap_{p|d} \mathcal{A}_p$.

- Set $\omega(1) = 1$ and $\mathcal{A}_1 = \mathcal{A}$.

Ex) Idea

$$S(A, P, z) = \sum_{n \in A} \left(\sum_{d | (n, P(z))} \mu(d) \right)$$

$$= \sum_{\substack{d \le x \\ d | P(z)}} \mu(d) \underbrace{\left(\sum_{\substack{n \in A \\ d | n}} 1 \right)}_{\# A_d}$$

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

In general

$$\boxed{S(A, P, z) = \sum_{\substack{d \le x \\ d | P(z)}} \mu(d) \# A_d}$$

Theorem (The sieve of Eratosthenes)

Suppose the following conditions hold:

- *There exists an X such that* $\boxed{\#\mathcal{A}_d = \frac{\omega(d)}{d}X + O(\omega(d)),}$ like $\lfloor \frac{x}{d} \rfloor = \frac{x}{d} + O(1)$
- *For some* $\kappa \geqslant 0$,

$$\sum_{p \mid P(z)} \frac{\omega(p)\log p}{p} \leqslant \kappa \log z + O(1),$$

- *For some* $y > 0$, $\#\mathcal{A}_d = 0$ *for every* $d > y$.

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

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

Instead of $\displaystyle\sum_{\substack{d \le x \\ d \mid P(z)}} 1 \ll \Psi(x,z)$

use $\displaystyle\sum_{\substack{d \le x \\ d \mid P(z)}} w(d) := F_w(x,z)$

Brun's Sieves

Brun's sieve is set up in essentially the same way as Eratosthenes. Given some set $\mathcal{A}$ of integers $\leqslant x$, we have some collection of $\mathcal{A}_p$ of elements we want to remove, and measure the size of

$$S(\mathcal{A},\mathcal{P},z) = \#\left(\mathcal{A}\backslash \bigcup_{p|P(z)} \mathcal{A}_p\right).$$

Idea (Punchline of Brun's results)

Under similar, but slightly relaxed, hypotheses to the sieve of Eratosthenes, Burn proves that

$$S(\mathcal{A},\mathcal{P},z) = XW(z) + O\left(\textit{better error}\right)$$

where $X = \#\mathcal{A}$ *and*

$$W(z) = \prod_{p|P(z)} \left(1 - \frac{\omega(p)}{p}\right).$$

Theorem (Brun's Pure Sieve)

Suppose the following conditions hold:

like $\lfloor \frac{x}{d} \rfloor = \frac{x}{d} + O(1)$

- *There exists an X such that* $\boxed{\#\mathcal{A}_d = \frac{\omega(d)}{d}X + O(\omega(d)),}$
- *There exists a constant C such that* $\omega(p) < C$,
- *There exist constants C_1 and C_2 such that*

$$\sum_{p | P(z)} \frac{\omega(p)}{p} \leqslant C_1 \log\log z + C_2,$$

Then

$$S(\mathcal{A}, \mathcal{P}, z) = \underbrace{XW(z)}_{\text{main term}} + \underbrace{XW(z)O\left((\log z)^{-\eta \log \eta}\right) + O\left(z^{\eta \log\log z}\right)}_{\text{error terms}}$$

where η is any positive number (possibly depending on x and z.)

$$\boxed{\log z = \frac{\log x}{A \log\log x}}$$

$$z^{\eta \log\log z} = \exp(\eta \log z \log\log z) = \exp\left(\frac{\eta \log x}{A \log\log x}(\log\log x - \log A - \log\log\log x)\right)$$

$$= x^{\frac{\eta}{A} - \frac{\eta \log A}{A \log\log x} - \frac{\eta \log\log\log x}{A \log\log x}} \ll x^{\frac{\eta}{A}}$$

small if A is large

Theorem

$$\#\{p \leqslant x : p \text{ and } p+2 \text{ are prime}\} \ll \frac{x(\log\log x)^2}{(\log x)^2}.$$

compare with $\pi(x) \sim \frac{x}{\log x}$

$$\boxed{\log z = \frac{\log x}{A \log\log x}}$$

$z = \exp\left(\frac{\log x}{A \log\log x}\right)$

Df $A_p = \{n \leq x : n \equiv 0 \text{ or } -2 \bmod p\}$

i.e. $p \mid n$ or $p \mid n+2$

$$S(A,P,z) \ll x \prod_{p<z}\left(1 - \frac{2}{p}\right)$$

$1 + x \leq e^x$

$$\ll x \exp\left(-2 \sum_{p<z} \frac{1}{p}\right)$$

$$\ll \frac{x}{(\log z)^2} = \frac{x A^2 (\log\log x)^2}{(\log x)^2}$$

main $\quad \ll x^{1/2}$

$$\#\{p \leq x : p, p+2 \text{ prime}\} \leq S(A,P,z) + \pi(z) \ll \boxed{\frac{x(\log\log x)^2}{(\log x)^2}} + \boxed{x^{\frac{1}{A \log\log x}}}$$

error

Corollary

$$\sum_{\substack{p \\ p+2 \text{ prime}}} \frac{1}{p} < \infty.$$

$\sum_p \frac{1}{p}$ diverges

Abel summation

$a_n = \begin{cases} 1 & n, n+2 \text{ prime} \\ 0 & \text{else} \end{cases}$

$f(t) = \frac{1}{t}$

$f'(t) = -\frac{1}{t^2}$

$A(t) = \#\{p \le x : p, p+2 \text{ prime}\}$

$$\sum_{\substack{p > 1.5 \\ p+2 \text{ prime}}} \frac{1}{p} = \frac{A(t)}{t}\Big|_{1.5}^{\infty} + \int_{1.5}^{\infty} \frac{A(t)}{t^2}\, dt$$

$$\ll \lim_{b\to\infty} \frac{(\log\log b)^2}{(\log b)^2} + O(1) + \int_{1.5}^{\infty} \frac{(\log\log t)^2}{t(\log t)^2}\, dt$$

$u = \log t$

$du = \frac{dt}{t}$

$$\ll 0 + O(1) + \int_{\log 1.5}^{\infty} \frac{(\log u)^2}{u^2}\, du$$

converges by comparison with $\int \frac{1}{u^{3/2}}\, du$

The big idea: **truncated Möbius Inversion**

Lemma

Let n and r be positive integers with $r \leqslant \nu(n) = \#\{\text{distinct prime divisors of } n\}$. There exists $|\theta| \leqslant 1$ such that

$$\sum_{d|n} \mu(n) = \sum_{\substack{d|n \\ \nu(d)\leqslant r}} \mu(d) + \theta \left(\sum_{\substack{d|n \\ \nu(n)=r+1}} \mu(d) \right)$$

- $\displaystyle\sum_{d|P(z)}$ has 2^z terms
- $\displaystyle\sum_{\substack{d\leq x \\ d|P(z)}}$ has $\ll x \log z \exp\left(-\frac{\log x}{\log z}\right)$ terms
- $\displaystyle\sum_{\substack{d|P(z) \\ \nu(d)\leq r}}$ has $\ll z^r$ terms

Pf $$\sum_{\substack{d|n \\ \nu(d)\le r}} \mu(d) = 1 + \sum_{p|n}(-1) + \sum_{p_1p_2|n}(-1)^2 + \cdots + \sum_{p_1\cdots p_r|n}(-1)^r$$

$$= 1 + \binom{\nu(n)}{1}(-1) + \binom{\nu(n)}{2}(-1)^2 + \cdots + \binom{\nu(n)}{r}(-1)^r$$

$$= \sum_{k=0}^{r} \binom{\nu(n)}{k}(-1)^k$$

$$= \binom{\nu(n)-1}{r}(-1)^r \quad \underline{\text{exercise}}$$

$$\sum_{\substack{d|n \\ \nu(d)\le 2r+1}} \mu(d) \le \sum_{d|n}\mu(d) \le \sum_{\substack{d|n \\ \nu(d)\le 2r}} \mu(d)$$

$$\sum_{\substack{d|n \\ \nu(d)=2r+1}} \mu(d) \le \sum_{d|n}\mu(d) - \sum_{\substack{d|n \\ \nu(d)\le 2r}} \mu(d) \le 0$$

$\square$

$$S(A,P,z) = \sum_{a\in A}\left(\sum_{d\mid (a,P(z))}\mu(d)\right)$$

[choose $r = \lfloor \eta \log\log x \rfloor$]

$$= \sum_{d\in A}\left(\sum_{\substack{d\mid (a,P(z))\\ \nu(d)\le r}}\mu(d) + \theta \sum_{\substack{d\mid (a,P(z))\\ \nu(d)=r+1}}\mu(d)\right)$$

$$= \sum_{\substack{d\mid P(z)\\ \nu(d)\le r}}\mu(d)\,\#A_d + O\left(X\,\frac{\pi(z)^{r+1}}{(r+1)!}\right)$$

$\#A$

$\#d\mid P(z)$, $\nu(d)=r+1$

choosing $r+1$ primes from $\pi(z)$ primes $= \binom{\pi(z)}{r+1}$

$$= X\sum_{d\mid P(z),\ \nu(d)\le r}\mu(d)\,\frac{\omega(d)}{d} + O\left(\sum_{\substack{d\mid P(z)\\ \nu(d)\le r}}\omega(d)\right) + O\left(X\,\frac{z^{r+1}}{(r+1)!}\right)$$

The big idea: **Replace Möbius sums with an apporximation**

$$\sum_{d|n} \mu(d) \leftrightarrow \sum_{d|n} \mu(d) g(d)$$

Strategic choices of “lower” and “upper” weight functions give bounds

$$\sum_{d|P(z)} \mu(d) g_L(d) \# \mathcal{A}_d \leqslant S(\mathcal{A}, \mathcal{P}, z) \leqslant \sum_{d|P(z)} \mu(d) g_U(d) \# \mathcal{A}_d$$

which are easier to count.

Idea (Brun's Main Theorem)

There exist constants c_1 and c_2 such that

$$S(\mathcal{A}, \mathcal{P}, z) \leqslant c_1 X W(z) + O\left(z^{\theta}\right)$$

and

$$S(\mathcal{A}, \mathcal{P}, z) \geqslant c_2 X W(z) + O\left(z^{\theta-1}\right),$$

where θ is given explicitely.

can choose $z = x^{\frac{1}{\theta} - \varepsilon}$

earlier $\log z = \frac{\log x}{A \log\log x} \Rightarrow z = x^{\frac{1}{A\log\log x}}$