Lecture 7

The Selberg Sieve

Let $h \in \mathbb{Z}[n]$, $\mathcal{A} = \{h(n) : x_0 < n \leq x_0 + x\}$, $\mathcal{P} = \{\text{all primes}\}$ and $z > 0$.

We wish to find upper bounds on the number of primes in $\mathcal{A}$, which we shall do by estimating $S(\mathcal{A}, \mathcal{P}, z)$, the number of elements in $\mathcal{A}$ which are <u>not</u> divisible by any $p \leq z$.

If for squarefree integers d (the case of interest to us) we denote by $v(d)$ the number of elements of $\{h(1), \dots, h(d)\}$ that are divisible by d, then it is easy to see that

$$A_d := \#\{a \in A : d \mid a\} = x\frac{v(d)}{d} + r_d \quad , \text{with } |r_d| \leq v(d).$$

and that v may be extended to be <u>completely multiplicative</u> on $\mathbb{N}$.

<u>Theorem 1</u>: $$S(A, \mathcal{P}, z) \leq x\left(\sum_{d \leq z} \frac{v(d)}{d}\right)^{-1} + z^2 \prod_{p \leq z}\left(1 - \frac{v(p)}{p}\right)^{-2}.$$

<u>Exercise 1</u>: Show that if $v(p) \leq B$ for all $p \leq z$, then

$$\prod_{p \leq z}\left(1 - \frac{v(p)}{p}\right)^{-1} \ll (\log z)^B$$

<u>Hint</u>: Show that $\left(1 - \frac{B}{p}\right) \geq \left(1 - \frac{1}{p}\right)^B\left(1 - \frac{B}{p^2}\right)$ for suff. large p, then use Mertens.

Applications

1. Primes in an Interval:

Let $h(n) = n$, then $\nu(p) = 1$ for all $p \geq 2$ and Theorem 1 implies that

$$S(\mathcal{A}, \mathcal{P}, z) \leq \frac{x}{\log z} + O(z^2 (\log z)^2)$$

for all $z > 0$, since $\sum_{d \leq z}' \frac{1}{d} \geq \log z$ and by Mertens we know that

$$\prod_{p \leq z} \left(1 - \frac{1}{p}\right)^{-1} \ll \log z .$$

Since

$$\pi(x_0 + x) - \pi(x_0) \leq z + S(\mathcal{A}, \mathcal{P}, z)$$

for all $z > 0$, the following result follows by taking $z = \frac{x^{1/2}}{(\log x)^2}$ (Check!!)

Theorem 2 (Brun–Titchmarsh) For any x_0

$$\pi(x_0 + x) - \pi(x_0) \leq \frac{(2 + \varepsilon(x))\, x}{\log x}$$

where $\varepsilon(x) \to 0$ as $x \to \infty$.

2. Twin Primes:

Let $h(n) = n(n+2)$, then $\nu(p) = \begin{cases} 1 & \text{if } p = 2 \\ 2 & \text{if } p \geq 3 \end{cases}$.

divisors of d.

To bound $\sum_{d \leq z}' \frac{\nu(d)}{d}$ from below we observe that

$$\nu(d) \geq \tau(d) \text{ for all } d \text{ odd}.$$

This follows by writing $d = p_1^{l_1} \cdots p_k^{l_k}$, so that $v(d) = 2^{l_1} \cdots 2^{l_k}$ and $\tau(d) = (l_1+1)\cdots(l_k+1)$. From this observation it follows that

$$\sum_{\substack{d \le z \\ d \text{ odd}}} \frac{v(d)}{d} \geq \sum_{\substack{d \le z \\ d \text{ odd}}} \frac{\tau(d)}{d} \geq \Big(\sum_{\substack{d \le \sqrt{z} \\ d \text{ odd}}} \frac{1}{d} \Big)^2 \gg (\log z)^2 .$$

Since Exercise 1 implies that $\prod_{p \le z} \left(1 - \frac{v(p)}{p}\right)^{-1} \ll (\log z)^2$, it follows from Theorem 1 that

$$S(\mathcal{A}, \mathcal{P}, z) \ll \frac{x}{(\log z)^2} + z^2 (\log z)^4$$

for all $z > 0$. Since $\pi_2(x) \le z + S(\mathcal{A}, \mathcal{P}, z)$ for all $z > 0$, taking $\underline{z = x^{1/3}}$ gives:

<u>Theorem 3</u>: $\quad \pi_2(x) \ll \dfrac{x}{(\log x)^2}$.

<u>3. Goldbach Problem</u>:

Let $h(n) = n(N-n)$ for a given $N \in \mathbb{N}$. It is easy to see that in this case

$$v(p) = \begin{cases} 1 & \text{if } p \mid N \\ 2 & \text{if } p \nmid N \end{cases} \qquad (\underline{\text{Check}}!!)$$

Once again we will apply Theorem 1. To bound $\sum_{d \le z} \frac{v(d)}{d}$ from below this time suppose $d = p_1^{l_1} \cdots p_k^{l_k} q_1^{m_1} \cdots q_r^{m_r}$, where $p_i \mid N$ and $q_j \nmid N$.

The $v(d) = 2^{m_1} \cdots 2^{m_r}$, which is at least $(m_1+1)\cdots(m_r+1)$, namely the number of divisors of d that are relatively prime to N. It follows that

$$\sum_{d \le z}' \frac{v(d)}{d} \geqslant \left(\sum_{m \le \sqrt{z}} \frac{1}{m} \right) \left(\sum_{\substack{n \le \sqrt{z} \\ (n,N)=1}} \frac{1}{n} \right).$$

From the easily verified fact that

$$\left(\sum_{\substack{n \le \sqrt{z} \\ (n,N)=1}} \frac{1}{n} \right) \cdot \prod_{p \mid N} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots \right) \gg \sum_{n \le \sqrt{z}} \frac{1}{n} \gg \log z$$

we see that

$$\sum_{d \le z}' \frac{v(d)}{d} \gg (\log z)^2 \prod_{p \mid N} \left(1 - \frac{1}{p}\right).$$

Since $\dfrac{1 - \frac{1}{p^2}}{1 - \frac{1}{p}} = 1 + \frac{1}{p}$ and $\prod\limits_{p \mid N}\left(1 - \frac{1}{p^2}\right)$ converges, and the fact that

$$R(N) := \#\{ (p_1, p_2) \in \mathcal{P}^2 : p_1 + p_2 = N \} \leqslant S(A, \mathcal{P}, z) + 2z$$

Why?

for all $z > 0$, taking $z = N^{1/3}$ in Theorem 1 gives:

<u>Theorem 4</u>: $$R(N) \ll \frac{N}{(\log N)^2} \prod_{p \mid N} \left(1 + \frac{1}{p}\right).$$

<u>Exercise 2</u>: Prove the following generalization of Theorem 3:

<u>Theorem 5</u>: If $\pi_m(x) := \#\{ n \le x : n \;\&\; n+m \text{ prime} \}$, then

$$\pi_m(x) \ll \frac{x}{(\log x)^2} \prod_{p \mid m} \left(1 + \frac{1}{p}\right).$$

Proof of Theorem 1

Let $\lambda : \mathbb{N} \to \mathbb{R}$ be any function whatsoever with $\lambda(1)=1$. Then

$$\Big(\sum_{d|n} \lambda(d) \Big)^2 \begin{cases} =1 & \text{if } n=1 \\ \geq 0 & \text{if } n>1 . \end{cases}$$

This simple observation can be used to obtain upper bounds for $S(\mathcal{A},\mathcal{P},z)$, namely

$$S(\mathcal{A},\mathcal{P},z) \leq \sum_{a\in\mathcal{A}} \Big(\sum_{d|(a,P(z))} \lambda(d) \Big)^2 = \sum_{a\in\mathcal{A}} \sum_{\substack{d_1,d_2|a \\ d_1,d_2|P(z)}} \lambda(d_1)\lambda(d_2) = \sum_{d_1,d_2|P(z)} \lambda(d_1)\lambda(d_2) A_{[d_1,d_2]}$$

where $P(z) = \prod_{p\leq z} p$ & $[d_1,d_2] := \operatorname{lcm}(d_1,d_2)$.

Let us assume further that $\lambda(d)=0$ whenever $d \nmid P(z)$, then

$$S(\mathcal{A},\mathcal{P},z) \leq X \underbrace{\sum_{d_1,d_2|P(z)} \lambda(d_1)\lambda(d_2) \frac{\nu([d_1,d_2])}{[d_1,d_2]}}_{=Q} + \underbrace{\sum_{d_1,d_2|P(z)} \lambda(d_1)\lambda(d_2) r_{[d_1,d_2]}}_{=R}$$

We shall see that if we further assume that $\lambda(d)=0$ for all $d>z$, then this will allow us to control R.

As for the main term Q, we see that we wish to minimize a quadratic form subject to the constraint $\lambda(1)=1$. It turns out that we can diagonalize this quadratic form and determine the optimal choice of function λ exactly.

We first diagonalize Q.

Since $\quad d_1 d_2 = [d_1, d_2](d_1, d_2)$ it follows that

$$\frac{v(d_1)v(d_2)}{d_1 \; d_2} = \frac{v([d_1,d_2])}{[d_1,d_2]} \frac{v((d_1,d_2))}{(d_1,d_2)}$$

and hence that

$$\overset{?}{=} \sum_{k \mid (d_1,d_2)} f(k) \text{ for some } f$$

$$Q = \sum_{d_1, d_2 \mid P(z)} \lambda(d_1)\lambda(d_2) \frac{v(d_1)v(d_2)}{d_1 \; d_2} \frac{(d_1,d_2)}{v((d_1,d_2))} .$$

[Let $g(n) = \dfrac{n}{v(n)}$, recall that by Möbius inversion

$$g(n) = \sum_{k \mid n} f(k) \iff f(n) = \sum_{k \mid n} \mu\left(\frac{n}{k}\right) g(k)$$]

Thus,

$$Q = \sum_{k \mid P(z)} f(k) \sum_{\substack{d_1, d_2 \mid P(z) \\ k \mid d_1, d_2}} \frac{\lambda(d_1)v(d_1)}{d_1} \cdot \frac{\lambda(d_2)v(d_2)}{d_2} = \sum_{k \mid P(z)} f(k) y(k)^2$$

where

$$y(k) = \sum_{\substack{d \mid P(z) \\ k \mid d}} \frac{\lambda(d)v(d)}{d} \quad \& \quad f(k) = \sum_{d \mid k} \mu\left(\frac{k}{d}\right) \frac{d}{v(d)} .$$

<u>Exercise</u> (3): Show that

$$y(k) = \sum_{\substack{d \mid P(z) \\ k \mid d}} \frac{\lambda(d)v(d)}{d} \iff \lambda(k) = \frac{k}{v(k)} \sum_{\substack{d \mid P(z) \\ k \mid d}} \mu\left(\frac{d}{k}\right) y(d)$$

In particular,

$$\lambda(d) = 0 \;\; \forall\, d > z \iff y(d) = 0 \;\; \forall\, d > z .$$

We have therefore diagonalized Q and by Exercise 3 we see that the constraint

$$\lambda(1)=1 \iff \sum_{k|P(z)} \mu(k)y(k)=1.$$

Notice that if $\sum_{k|P(z)} \mu(k)y(k)=1$, then

$$Q=\sum_{k|P(z)} f(k)y(k)^2=\sum_{\substack{k|P(z)\\ k\le z}} f(k)\left(y(k)-\frac{\mu(k)}{f(k)D(z)}\right)^2+\frac{1}{D(z)}$$

where

$$D(z)=\sum_{\substack{d|P(z)\\ d\le z}} 1/f(d).$$

It follows that the minimum value of Q is $1/D(z)$ and that this occurs when $y(k)=\mu(k)/f(k)D(z)$. In otherwords, we have found our optimal function λ with $\lambda(1)=1$, namely

$$\lambda(k)=\frac{k}{v(k)}\sum_{\substack{d|P(z)\\ k|d\\ d\le z}} \mu\left(\frac{d}{k}\right)\mu(d)/f(d)D(z).$$

Notice that

$$|\lambda(k)|\le\frac{k}{v(k)D(z)}\sum_{\substack{d|P(z)\\ k|d\\ d\le z}}\frac{1}{f(d)}\le\frac{k}{v(k)D(z)}\frac{1}{f(k)}\sum_{\substack{m|P(z)\\ m\le z}}\frac{1}{f(m)}=\frac{k}{v(k)f(k)}$$

Here we have used the multiplicativity of $f(d):=\sum_{k|d}\mu\left(\frac{d}{k}\right)\frac{k}{v(k)}$.

It follows, since $v((d_1,d_2)) \geqslant 1$, that

$$|R| \leqslant \sum_{d_1,d_2 \mid P(z)}' |\lambda(d_1)||\lambda(d_2)| \, v([d_1,d_2])$$

$$\leqslant \Big(\sum_{d \mid P(z)}' |\lambda(d)| \, v(d) \Big)^2 \leqslant \Big(\sum_{\substack{d \mid P(z) \\ d \leq z}} \frac{\kappa}{f(\kappa)} \Big)^2 \leqslant z^2 \, D(z)^2 .$$

We have now established that for all $z > 0$

$$S(\mathcal{A}, \mathcal{P}, z) \leq X \frac{1}{D(z)} + z^2 D(z)^2 , \quad D(z) = \sum_{\substack{d \mid P(z) \\ d \leq z}} 1/f(d) .$$

To complete the proof of Theorem 1, we must show:

$$\sum_{d \leq z} \frac{v(d)}{d} \underset{\text{(i)}}{\leqslant} D(z) \underset{\text{(ii)}}{\leqslant} \prod_{p \leq z} \Big(1 - \frac{v(p)}{p}\Big)^{-1}$$

Key to both these estimates is the multiplicativity of f & $f(p) = \frac{p}{v(p)} - 1$.

<u>(i)</u>:
$$\sum_{\substack{d \mid P(z) \\ d \leq z}} \frac{1}{f(d)} = \sum_{\substack{d \leq z \\ \mu(d) \neq 0}} \prod_{p \mid d} \frac{v(p)/p}{1 - v(p)/p} = \sum_{\substack{d \leq z \\ \mu(d) \neq 0}} \prod_{p \mid d} \Big(\frac{v(p)}{p} + \frac{v(p^2)}{p^2} + \cdots \Big) \geqslant \sum_{d \leq z} \frac{v(d)}{d} .$$

<u>(ii)</u>:
$$\sum_{\substack{d \mid P(z) \\ d \leq z}} \frac{1}{f(d)} \leqslant \prod_{p \leq z} \Big(1 + \frac{1}{f(p)}\Big) \leqslant \prod_{p \leq z} \Big(1 - \frac{v(p)}{p}\Big)^{-1} .$$

$\square$