Thm 11.3.5 (Fundamental lemma of sieve theory)

Let $a_1, a_2, \dots$ be a mult. seq. of sieve dimension $\leq K$.

Let $s \geq 1$ be suff. large (depending on the sequence).

Let $D \geq 1$ and $z = D^{1/s}$.

For some $1 \leq \beta \leq s$, we then have

$$\sum_{d \in \mathcal{D}^{\pm}_{\beta,D}} \mu(d) a_d = V(z) \left(1 + O(e^{-s})\right).$$

(In part., for large s,

$$\sum_{\sim} \mu(d) a_d \asymp V(z).\ )$$

Lemma 11.3.6

If $d = p_1 \cdots p_r \in \mathcal{Q}^{\pm}_{\beta,D}$ with $p_1 < \dots < p_r < D^{1/\beta}$,
then $d \le D^{1-\left(\frac{\beta-1}{\beta}\right)^r}$.

Pf by ind. over r.

$r=0$: $d=1$ $\le D^{1-1}$ ✓

$r=1$: $d = p_1 < D^{1/\beta} = D^{1-\frac{\beta-1}{\beta}}$ ✓

$r \ge 2$: We have

$$p_k^{\beta+1} p_{k+1} \cdots p_r \le D \text{ for } k=1 \text{ or for } k=2$$

(depending on the parity of r).

$$\Rightarrow p_1^{\beta} p_2 \cdots p_r \le D. \qquad (I)$$

Since $p_2 \cdots p_r \in \mathcal{Q}^{\pm}_{\beta,D}$ according to axiom b),

we have $p_2 \cdots p_r \le D^{1-\left(\frac{\beta-1}{\beta}\right)^{r-1}}$ by induction.

$$\Rightarrow d^{\beta} = (p_1 \cdots p_r)^{\beta} \underset{(I)}{\le} D \cdot (p_2 \cdots p_r)^{\beta-1}$$

$$\le D^{1+(\beta-1)\left(1-\left(\frac{\beta-1}{\beta}\right)^{r-1}\right)} = D^{\beta\left(1+\left(\frac{\beta-1}{\beta}\right)^r\right)}.$$

□

Pf of Thm 11.3.5

$$\sum_{d \in \mathcal{D}^{\pm}_{\beta,D}} \mu(d)\, a_d$$

$$= \text{(Lemma 11.3.2)} \quad V(z) + \mathcal{O}\Big(\sum_{\substack{d \in \mathcal{D}_0 : \\ d \notin \mathcal{D}^{\pm}_{\beta,D} \\ \frac{d}{\mathrm{lpf}(d)} \in \mathcal{D}^{\pm}_{\beta,D}}} a_d \, V(\mathrm{lpf}(d)) \Big)$$

$$\ll V(z) \cdot \left(\frac{\log(z)}{\log(\mathrm{lpf}(d))} \right)^k$$

Write $d = p_1 \cdots p_r$.

If $d \notin \mathcal{D}^{*}_{\beta,D}$, (but $\frac{d}{p_1} \in \mathcal{D}^{\pm}_{\beta,D}$) we must have $D^{\frac{\beta+r}{s}} \geq p_1^{\beta+1} p_2 \cdots p_r > D$,

so $r > s - \beta$. Moreover, by Lemma 11.3.6, we have

$p_2 \cdots p_r \leq D^{1-\left(\frac{\beta-1}{\beta}\right)^{r-1}}$, so then

$$p_1^{\beta+1} > D^{\left(\frac{\beta-1}{\beta}\right)^{r-1}} > D^{\left(\frac{\beta-1}{\beta}\right)^{r} \cdot \frac{\beta+1}{\beta}}$$

, so

$$p_1 > D^{\left(\frac{\beta-1}{\beta}\right)^{r} \cdot \frac{1}{\beta}} \geq z^{\left(\frac{\beta-1}{\beta}\right)^{r}}.$$

($D = z^s$, $s \geq \beta$)

In particular, $\frac{\log z}{\log p_1} \leq \left(\frac{\beta}{\beta-1}\right)^{r}$

$$\Rightarrow A := \frac{\sum_{d \in \mathcal{Q}^*_{\beta,D}} \mu(d) a_d}{V(z)} - 1$$

$$\ll \sum_{d = p_1 \cdots p_r} a_d \cdot \left(\frac{\beta}{\beta-1}\right)^{r\kappa}$$

$$z^{\left(\frac{\beta-1}{\beta}\right)^r} \le p_1 < \ldots < p_r < z$$

$$r > s - \beta$$

$$\le \sum_{r > s-\beta} \frac{1}{r!} \Bigg(\underbrace{\sum_{z^{\left(\frac{\beta-1}{\beta}\right)^r} \le p < z} a_p}_{\ll 1} \Bigg)^r \cdot \left(\frac{\beta}{\beta-1}\right)^{r\kappa}$$

$$-\log \frac{V(z)}{V\left(z^{\left(\frac{\beta-1}{\beta}\right)^r}\right)} \le \{ r \kappa \log \frac{\beta}{\beta-1} + O(1) \}$$

$$\le \sum_{r > s-\beta} \underbrace{\frac{r^r}{r!}}_{\le e^r} \cdot \left(\kappa \log \frac{\beta}{\beta-1} + O\left(\frac{1}{r}\right) \right)^r \cdot \left(\frac{\beta}{\beta-1}\right)^{r\kappa}$$

Let $f(\beta) = e^{\kappa} \log \frac{\beta}{\beta-1} \cdot \left(\frac{\beta}{\beta-1}\right)^{\kappa}$.

We have $f(\beta) \to 0$ as $\beta \to \infty$.

Choose β so that $f(\beta) \le \frac{1}{2e}$. Then,

$$A \ll \sum_{r \ge s-\beta} \left(\frac{1}{2e} + O_\beta\left(\frac{1}{r}\right) \right)^r \le \sum_{r \ge s-\beta} \frac{1}{e^r} \ll_\beta \frac{1}{e^s}.$$

(suff. large s)

□

Cor 11.3.7 (Weaker form of twin prime conjecture)

Let $t \geq 1$ be suff. large. Then, for large x, we have

$$N(x) := \#\left\{ n \leq x : \begin{array}{l} n, n+2 \text{ aren't divisible by} \\ \text{any } p \leq x^{1/t} \end{array} \right\} \gg \frac{x}{(\log x)^2}.$$

Rmk $\ll$ $n \leq x$ can be divisible by at most t primes $\leq x^{1/t}$.

Pf of Cor Let $D = x^{1/2}$, $z = D^{1/s} = x^{1/2s}$.

$(\rightsquigarrow t := 2s)$.

We've seen in the pf of Cor 11.2.3 that if

$$a_d = \begin{cases} \frac{z^{\nu(d)}}{d}, & d \text{ odd}, \\ 0, & d \text{ even}, \end{cases}$$

then

$$\#\{ n \leq x : d \mid (2n+1)(2n+3) \} = x \cdot a_d + O(z^{\nu(d)}).$$

$\Rightarrow$

$$N(x) \geq \sum_{d \in \mathcal{D}^-_{\beta,D}} \mu(d) \cdot \#\{ n \leq x : d \mid \dots \}$$

$$= x \sum_{d \in \mathcal{D}^-_{\beta,D}} \mu(d) \cdot a_d + O\Big(\underbrace{\sum_{d \in \mathcal{D}^-_{\beta,D}} z^{\nu(d)}}_{\leq \sum_{d \leq D} z^{\nu(d)}} \Big)$$

$$\asymp D \log D$$

$$\asymp x^{1/2} \log x$$

Also,

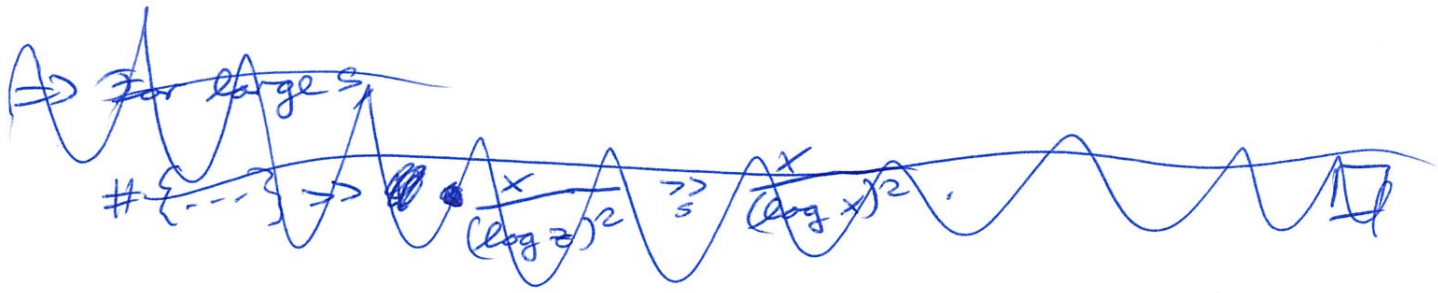
$$\sum_{d \in \mathcal{D}_{\beta,D}} \mu(d) \cdot a_d \asymp V(z) \quad \text{for large } s$$

$$\| \quad \text{and appropriate } \beta.$$

$$\prod_{2<p<z} \left(1 - \frac{2}{p}\right) \asymp (\log z)^{-2} \asymp (\log x)^{-2}$$

for fixed s.

$$\Rightarrow N(x) \gg \frac{x}{(\log x)^2} + O(x^{1/2} \log x) \gg \frac{x}{(\log x)^2}. \qquad \square$$



Rmk Using more advanced sieves, Chen proved that

~~there are suff. large~~

~~every suff. large even n is the sum~~

there are ∞ many primes p such that $p+2$ is prime or the product of two primes.

Rmk Using a very different method (more like Selberg sieves), Zhang showed that there are ∞ many pairs of primes of bounded distance. ($\leq B$)

Better result with simpler proof: Maynard, Small gaps between primes

Idea: Find a ~~[illegible]~~ sequence $\nu_1, \nu_2, \dots \geq 0$ such that

$$\sum_{i=0}^{B} \sum_{\substack{\frac{x}{2} < n \leq x \\ n+i \text{ prime}}} \nu_n > \sum_{\frac{x}{2} < n \leq x} \nu_n \quad \text{for all suff. large } x. \qquad (\mathrm{I})$$

Then, for some $\frac{x}{2} < n \leq x$, there must be $0 \leq i_1 < i_2 \leq B$ with $n+i_1, n+i_2$ both prime. To ensure (I), one should choose ~~[illegible]~~ $(\nu_n)_n$ ~~[illegible]~~ so that ~~[illegible]~~ ν_n tends to be larger ~~when [illegible]~~ the more of the numbers $n+i$ $(0 \leq i \leq B)$ are prime, but so that we can still bound $\sum_{\substack{n: \\ n+i \text{ prime}}} \nu_n$ from below effectively.

(Essentially, they take $\nu_n = [illegible]\left(\sum_{\substack{d_0 \mid n \\ d_1 \mid n+1 \\ \vdots \\ d_B \mid n+B}} \mu(d_0)\cdots\mu(d_B) f\left(\frac{\log d_0}{\log [illegible]}, \ldots, \frac{\log d_B}{\log [illegible]}\right)\right)^2$

for a suitable [illegible] smooth compactly supported function

$f : \mathbb{R}^{B+1} \longrightarrow \mathbb{R}$.)

11.4. Large sieve

In the previous applications, we've been forbidding only $O(1)$ residue classes mod each prime p.
What if we instead forbid a large number of residue classes? (say $\asymp p$ many.)

Reminder $c : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ any function

has Fourier transform $\hat{c} : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$

$$\hat{c}(t) = \sum_{x \in \mathbb{Z}/q\mathbb{Z}} c(x) e^{2\pi i x t/q}$$

$$q \cdot \sum_{x \in \mathbb{Z}} c(x \bmod q) f(x) = \sum_{t \in \mathbb{Z}} \hat{c}(t \bmod q) \hat{f}\left(\frac{t}{q}\right)$$

Lemma 11.4.1 $\sum_t \hat{c}(t)\overline{\hat{d}(t)} = q \sum_x c(x)\overline{d(x)}$, so in part. $\sum_t |\hat{c}(t)|^2 = q \cdot \sum |c(x)|^2$

Pf HW. □

Lemma 11.4.2 Let p be a prime and $c : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ a function which vanishes on (exactly) $w^{\in p}$ of the residue classes mod p.

Then, $\sum_{t \in (\mathbb{Z}/p\mathbb{Z})^\times} |\hat{c}(t)|^2 \geq \frac{w}{p-w} \cdot |\hat{c}(0)|^2$.

Pf $\sum_{t \in \mathbb{Z}/p\mathbb{Z}} |\hat{c}(t)|^2 = p \cdot \sum_{x \in \mathbb{Z}/p\mathbb{Z}} |c(x)|^2$

$$\hat{c}(0) = \sum_{x \in \mathbb{Z}/q\mathbb{Z}} c(x).$$

Let $d(x) = \begin{cases} 1, & c(x) \neq 0 \\ 0, & c(x) = 0. \end{cases}$

$c(x) = c(x) \cdot d(x)$