18.156, Projection theory, problem set 4

In this problem set, we digest the large sieve and its applications. First we recall the large sieve from class (Lecture 5). Recall that $[N] = \{1, ..., N\}$. If $f : [N] \to \mathbb{C}$, and $q \in \mathbb{N}$, we define $\pi_q f : \mathbb{Z}_q \to \mathbb{C}$ by

$$\pi_q f(a) = \sum_{n \in a} f(n).$$

We let $P_M := \{p \text{ prime } | p \sim M\}$.

Theorem 1. *(Linnik large sieve) If $f : [N] \to \mathbb{C}$, and $M \leq N^{1/2}$, then*

$$\sum_{p \in P_M} \|(\pi_p f)_h\|_{L^2}^2 \leq C \frac{N}{M} \|f\|_{L^2}^2.$$

1. In order to digest the proof of Theorem 1, sketch a proof for the following variation when $M > N^{1/2}$. This variation comes up in applications, like in the Bombieri-Vinogradov theorem.

Theorem 2. *(Linnik large sieve) If $f : [N] \to \mathbb{C}$, and $M > N^{1/2}$, then*

$$\sum_{p \in P_M} \|(\pi_p f)_h\|_{L^2}^2 \leq CM \|f\|_{L^2}^2.$$

In your proof sketch, describe the Fourier analysis technical details in the level of detail that you find most helpful. Your proof sketch should illustrate why we have a factor M on the right hand side in Theorem 2 as opposed to a factor of N/M in Theorem 1.

Linnik developed the large sieve to prove an estimate related to the distribution of quadratic residues. Our second goal for the problem set is to prove Linnik's result.

Background on quadratic residues. Suppose that p is a prime. Recall that a number $a \in \mathbb{Z}_p$ is called a quadratic residue if there is a solution to the equation $b^2 = a$ in $\mathbb{Z}_p$. (Here we count 0 as a quadratic residue, although sometimes one restricts attention to non-zero quadratic residues.) There are $\frac{p+1}{2}$ quadratic residues in $\mathbb{Z}_p$ and $\frac{p-1}{2}$ quadratic non-residues. Linnik wanted to understand how the quadratic residues are distributed in $\mathbb{Z}_p$. It appears that quadratic residues are distributed fairly randomly.

Suppose we took a large prime p and colored the quadratic residues in $\mathbb{Z}_p$. Then for comparison suppose we randomly colored $\mathbb{Z}_p$ in two colors. These two colorings would look pretty similar. In the random coloring, the longest string of consecutive numbers that are the same color would have length around $\log p$. Something like this appears to be true for quadratic residues as well.

Define $q(p)$ to be the smallest a so that a is a quadratic non-residue in $\mathbb{Z}_p$. (The smallest quadratic residue is always 0.) If $q(p)$ is large, then it means that there are many quadratic non-residues in a row. Experiments suggest that $q(p)$ is always $\lesssim \log p$ or so. The general Riemann hypothesis implies that $q(p) \lesssim (\log p)^2$. However, the best proven bound is much worse, roughly $q(p) \lesssim p^{0.15...}$.

Linnik proved that, while there may be a few primes with $q(p)$ very large, these primes are quite rare. Let us make a little notation. We define

$$P_{N^{1/2},L} := \{p \text{ prime} | p \sim N^{1/2}, q(p) > L\} \tag{1}$$

Then we define

$$X_{N,L} := \{n \in \mathbb{N} | n \leq N, \text{ each prime factor of } n \text{ is at most } L\} \tag{2}$$

Theorem 3. *(Linnik) There is a universal constant $C > 0$ so that*

$$|P_{N^{1/2},L}| \leq C \frac{N}{X_{N,L}}$$

Number theorists have a good sense of $|X_{N,L}|$. For instance, for any $\epsilon > 0$, as $N \to \infty$, $|X_{N,N^\epsilon}| \sim C(\epsilon)N$, for some $C(\epsilon) > 0$. So Linnik's theorem implies that $|P_{N^{1/2},N^\epsilon}| \leq C(\epsilon)$ uniformly in N.

In the rest of the problem set, you will prove Theorem 3.

2. Prove that if $p \in P_{N^{1/2},L}$, then $|\pi_p(X_{N,L})| \leq \frac{p+1}{2}$.

3. Suppose that $X \subset [N]$. Suppose that for some p, $|\pi_p(X)| \leq (0.99)p$. Prove that there is a constant $c > 0$ so that

$$\|(\pi_p 1_X)_h\|_{L^2}^2 \geq c\frac{|X|^2}{p}.$$

4. Prove Theorem 3 using the large sieve and problems 1,2.

Optional exploration. To pursue this direction, it would be helpful to have a little background in restriction theory in Fourier analysis, but anyone can understand the problem.

In class, we used the large sieve to prove the following estimate.

Theorem 4. *If $X \subset [N]$ and $|\pi_p(X)| \leq (0.99)p$ for every $p \in P_{N^{1/2}}$, then $|X| \lessapprox N^{1/2}$*

This theorem is essentially sharp when X is the set of squares.

We could explore what happens if we know $|\pi_p(X) \leq (0.99)p$ for every $p \in P_{N^\alpha}$ for some other exponent α, such as $\alpha = 1/4$.

Applying the large sieve as in Theorem 4 shows that, if $|\pi_p(X)| \leq (0.99)p$ for every $p \in P_{N^{1/4}}$, then $|X| \lessapprox N^{3/4}$. I don't know any example where this is roughly sharp, and I suspect there is no such example. Examining the proof of the large sieve, we see that if the bound is almost tight, then $\int_0^1 |\hat{1}_X(\xi)|^2 d\xi$ must be dominated by ξ very close to fractions of the form $\frac{a}{p}$, $p \in P_{N^{1/4}}$, $a \neq 0$. The region close to these fractions has a very small measure, around $N^{-1/2}$, so it is striking for this region to contribute a large fraction of the integral.

There is a vague principle in Fourier analysis called the Heisenberg uncertainty principle, which says that it is difficult for both f and $\hat{f}$ to concentrate in a small region. (The uncertainty principle can be made precise in various ways.) Here, the set $X \subset [N]$ is a small fraction of $[N]$ (because we already know $|X| \lessapprox N^{3/4}$). And if the large sieve argument is near tight, then $\hat{1}_X$ concentrates in a small region near to the fractions a/p, with $p \in P_{N^{1/4}}$. I suspect that there is no such set X, and one might be able to prove it using ideas related to the Heisenberg uncertainty principle or to restriction theory.

18.156 Projection Theory
Spring 2025