# IST in Analytic Number Theory
# ISI Kolkata, December 2017

## 1. Large Sieve

Through the problems in this section you will learn about the large sieve. The problems are divided into three sections : preliminaries, the large sieve and applications.

### Preliminaries

**1. Fourier Transforms on Finite Commutative Groups.**

Let $G$ be a finite commutative group. A homomorphism from $G$ into $\mathbf{C}^*$ is called a character of $G$. Since $G$ is finite the image of any character of $G$ is in fact contained in $\mathbf{T}$, the subgroup of $\mathbf{C}^*$ comprising the complex numbers of absolute value 1. The set of the characters of $\hat{G}$ has a natural group structure and with this structure this set is called the dual group of $G$ or the character group of $G$ and is denoted by $\hat{G}$. The group $\hat{G}$ is a finite commutative group that is (non-canonically) isomorphic to $G$. The dual group of $\hat{G}$ is canonically isomorphic to $G$ by means of the map $g \mapsto ev_g$, where $ev_g(\chi) = \chi(g)$ is the evaluation map on $\hat{G}$.

1.1. For any finite commutative group $G$, show that $\sum_{g\in G} \chi(g) = 0$ when $\chi$ is a non-trivial element in $\hat{G}$ and and is $|G|$ when $\chi$ is the trivial element of $\hat{G}$. Apply this to calculate $\sum_{\chi\in\hat{G}} \chi(g)$, for any $g$ in $G$.

1.2 Let $V(G)$ be the set of complex valued functions on $G$. Then check that $V(G)$ has a natural structure of a $\mathbf{C}$-vector space and that the dimension of this is vector space is $|G|$. For any $f$ and $h$ in $V(G)$ we set $\langle f, g\rangle = \sum_{g\in G} f(g)\overline{h(g)}$. Check that $\langle , \rangle$ gives $V(G)$ the structure of a Hermitian inner product space over $\mathbf{C}$.

1.3 Verify that the characters of $G$ form an orthogonal basis for $V(G)$. For any $f$ in $V(G)$ and any character $\chi$ of $G$, we write $\widehat{f(\chi)}$ to denote the coefficient of $\chi$ when $f$ is expressed in this basis. Conclude the following relations.

$$\widehat{f(\chi)} = \frac{1}{|G|}\sum_{g\in G} f(g)\overline{\chi(g)}\ . \tag{1}$$

$$\sum_{\chi\in\hat{G}} |\widehat{f(\chi)}|^2 \ = \ \frac{1}{|G|}\sum_{g\in G} |f(g)|^2\ . \tag{2}$$

The second relation above is called the Plancherel formula for $G$.

**2. The Selberg-Beurling Function.**

Let $I = [a, b]$ be a compact interval in $\mathbf{R}$ and $\delta$ be a real number $> 0$. In this part we shall construct a complex valued function function $\phi$, called the Selberg- Beurling function, on $\mathbf{R}$ satisfying the following conditions.

$(i)$ The function $\phi$ is the restriction to the real line of an entire function. Moreover $\phi$ is in $\mathrm{L}^1(\mathbf{R})$ and satisfies $\phi(x) \geq \chi_I(x)$ for all $x$ in $\mathbf{R}$, where $\chi_I$ is the characteristic function of the interval $I$.

$(ii)$ The fourier transform $\hat{\phi}$ of $\phi$ is supported in $[-\delta, \delta]$.

$(iii)$ We have $\hat{\phi}(0) = b - a + \frac{1}{\delta}$.

We introduce the function $K(z) = \left(\frac{sin\pi z}{\pi z}\right)^2$, which is an entire function on the complex plane and satifies $K(z) = K(-z)$ for all complex numbers $z$.

2.1 Verify that $K(x)$, for $x$ in $\mathbf{R}$, is in $\mathrm{L}^1(\mathbf{R})$ and $\int_{\mathbf{R}} K(x)dx = 1$. Moreover that for all complex numbers $z$ we have

$$1 = \sum_{n\in\mathbf{Z}} K(z-n)\ . \tag{3}$$

*Hint.*— Note that $K(x)$ is the fourier tranform of the function on the real line given by $1 - |x|$ when $|x| \leq 1$ and 0 for all other $x$. Apply the Poisson summation formula for the second part.

2.2 Show that for any real number $x > 0$ we have the inequalities

$$\sum_{n\geq 0} \frac{1}{(x+n)^2} \geq \frac{1}{x} \geq \sum_{n\geq 1} \frac{1}{(x+n)^2}\ . \tag{4}$$

*Hint.*— First observe that for any integer $n \geq 0$ and $x > 0$ we have the inequalities

$$\frac{1}{(x+n)^2} \geq \frac{1}{(x+n)(x+n+1)} \geq \frac{1}{(x+n+1)^2} \ . \tag{5}$$

Sum these inequalities over $n \geq 0$ and evaluate the sum in the middle of the resulting relation.

For any complex number $z$ we define $\mathrm{sgn}(z)$ to be 1 when $\mathrm{Re}(z) \geq 0$ and to be $-1$ when $\mathrm{Re}(z) < 0$. With this notation we define $B(z)$ for any complex number $z$ by the relation

$$B(z) = 2zK(z) \ + \sum_{n \in \mathbf{Z}} \mathrm{sgn}(n) K(z-n) \ . \tag{6}$$

2.3 Show that $B(z)$ is an entire function that satisfies the following conditions.

$(i)$ We have that $B(z) + B(-z) = 2K(z)$ for all complex numbers $z$.

$(ii)$ $B(n) = \mathrm{sgn}(n)$ for all $n$ in $\mathbf{Z}$. We have $B(z) - 1 = 2zK(z) - 2\sum_{n \geq 1} K(z+n)$ when $\mathrm{Re}(z) \geq 0$. We have $B(z) + 1 = 2zK(z) + 2\sum_{n \geq 0} K(z-n)$ when $\mathrm{Re}(z) < 0$.

*Hint.*— For the second part of $(ii)$ subtract (3) from (6). For the third part, add.

$(iii)$ Using Problem 2.2 and $(ii)$ above deduce that $B(x) \geq \mathrm{sgn}(x)$ for all real numbers $x$.

$(iv)$ Show that $\int_{\mathbf{R}} (B(x) - \mathrm{sgn}(x)) dx = 1$ and hence that $B(x) - \mathrm{sgn}(x)$ is in $\mathrm{L}^1(\mathbf{R})$.

*Hint.*— If $f(x) = B(x) - \mathrm{sgn}(x)$ then by $(iii)$ above $f(x) \geq 0$. Check that $f(x) + f(-x) = B(x) + B(-x)$ for all $x \neq 0$ in $\mathbf{R}$. Conclude from $(i)$ above that $\int_{\mathbf{R}} f(x)dx = \int_{\mathbf{R}} K(x)dx = 1$.

$(iv)$ Show that there is a constant $C > 0$ such that $|B(z) - \mathrm{sgn}(z)| \leq \frac{Ce^{2\pi|\mathrm{Im}(z)|}}{1+|z|^2}$, for all complex numbers $z$.

*Hint.*— Let us first take up the case when $\mathrm{Re}(z) \geq 0$, $z \neq 0$. Show using the second part of $(ii)$ above that in this case

$$B(z) - \mathrm{sgn}(z) = (\sin \pi z)^2 \sum_{n \geq 0} \frac{1}{(z+n)^2(z+n+1)} \ . \tag{7}$$

and consequently that

$$|B(z) - \mathrm{sgn}(z)| \leq |\sin \pi z|^2 \sum_{n \geq 0} \frac{1}{|z+n|^3} \ . \tag{8}$$

Now note that $|\sin \pi z| \leq e^{\pi |\mathrm{Im} z|}$ for all complex numbers $z$. To bound the infinite series, divide it into two parts $n \leq 2|z|$ and $n > 2|z|$. In the first part, use $|z/(z+n)| \leq 1$ for $\mathrm{Re}(z) \geq 0$. In the

second part, use $|z+n| \geq n/2$. Conclude in this manner that the absolute value of the infinite series is $\leq C/(1+|z|^2)$ for some constant $C > 0$. For $\mathrm{Re}(z) < 0$, use the first case together with $(i)$ above and the triangle inequality.

2.4 Let $\delta$ be a real number $> 0$ and $f(z)$ be an entire function on the complex plane satifying $|f(z)| \leq \frac{Ce^{2\pi\delta|\mathrm{Im}(z)|}}{1+|z|^2}$, for all complex numbers $z$ and some constant $C > 0$. Show that the restriction of $f(z)$ to the real line is in $\mathrm{L}^1(\mathbf{R})$ and that the fourier transform of this restriction is supported in the interval $[-\delta, \delta]$.

*Hint.*— This is an exercise in contour integration. By changing the variable to $z/\delta$, we reduce to the case when $\delta = 1$. In this case to show that the fourier transform $\hat{f}(t)$ of the restriction of $f$ to the real line, which we still denote by $f$, vanishes for $t > 1$ consider, for a given $t > 1$, the integral of $f(z)e^{-2\pi izt}$ on the rectangular contour with vertices $A$, $-A$, $-A - iT$ and $A - iT$ for $A$ and $T > 0$. Using the given growth condition show that the integrals over the sides of the contour not lying on the $X$-axis go to 0 as $A$ and $T$ tend to $+\infty$ and conclude. When $t < -1$, use a similar contour but this time lying above the $X$-axis.

2.5 Recall that $I$ denotes the interval $[a, b]$ and that $\chi_I$ is the characteristic function of $I$. Verify that for any $\delta > 0$ we have $\chi_I(x) = \frac{1}{2}(\mathrm{sgn}((x-a)\delta) + \mathrm{sgn}((b-x)\delta))$ for all real $x$.

2.6 Using the preceding problems conclude that $\phi(z) = \frac{1}{2}(B((z-a)\delta) + B((b-z)\delta))$ satisfies the requirements for $\phi$ given at the head of this section.

*Hint.*— Verify $\phi(x) = \chi_I(x) + \frac{1}{2}(B((x-a)\delta) - \mathrm{sgn}((x-a)\delta)) + \frac{1}{2}(B((b-x)\delta) - \mathrm{sgn}((b-x)\delta))$, for all real $x$. Note that $\hat{\phi}(0) = \int_{\mathbf{R}} \phi(x)dx$.

**3. An Elementary Duality Principle.**

The following simple principle is useful in a number of contexts in analytic number theory, even outside the basic theory of the large sieve.

3.1 For any finite sequence $x$ of complex numbers $x_l$ indexed by a finite set $L$ we write $\|x\|^2$ to denote $\sum_{l\in L} |x_l|^2$. Let $I$ and $J$ be finite indexing sets and $\{c_{ij}\}$ be a sequence of complex numbers indexed by $I \times J$. Finally, let $M$ be a real number $> 0$. Then show that the following statements are equivalent.

$(i)$ $\sum_{j\in J} |\sum_{i\in I} a_i c_{ij}|^2 \leq M\|a\|^2$ for all sequences $\{a_i\}_{i\in I}$ of complex numbers .

$(ii)$ $|\sum_{(i,j)\in I\times J} a_i b_j c_{ij}|^2 \leq M\|a\|^2\|b\|^2$ for all sequences of complex numbers $\{a_i\}_{i\in I}$ and $\{b_j\}_{j\in J}$.

$(iii)$ $\sum_{i\in I} |\sum_{j\in J} b_j c_{ij}|^2 \leq M\|b\|^2$ for all sequences of complex numbers $\{b_j\}_{j\in J}$.

*Hint.*— To show $(i)$ implies $(ii)$ write $|\sum_{(i,j)\in I\times J} a_i b_j c_{ij}| \leq \sum_{j\in J} |b_j||\sum_{i\in I} a_i c_{ij}|$ and apply the Cauchy-Schwarz Inequality together with $(i)$. To show $(ii)$ implies $(i)$, apply $(ii)$ with $\overline{b_j} = \sum_{i\in I} a_i c_{ij}$. The equivalence of $(iii)$ with $(ii)$ follows on interchanging the roles of $i$ and $j$.

## The Large Sieve

The large sieve answers the following question. Suppose that $M$ and $N$ are integers with $N \geq 1$ and let $A$ be a subset of the integers in the interval $[M+1, M+N]$. For each prime number $p$ let $A_p$ be a subset of $\mathbf{Z}/p\mathbf{Z}$ that contains the reduction of $A$ modulo $p$ and let us write $|A_p| = v_p p$. Thus $0 < v_p \leq 1$. The question is to obtain an upper bound for $|A|$ in terms of the $v_p$ and $N$. This is answered by the following result.

THEOREM . — *With notation as above we have for any $Q \geq 1$ that*

$$|A| \;\leq\; \frac{N-1+Q^2}{\sum_{1\leq d\leq Q} \mu^2(d) \prod_{p|d} \left(\frac{1-v_p}{v_p}\right)} \,. \tag{9}$$

Note that $\mu^2(d)$ is 1 when $d$ is square free and is 0 for all other integers $d \geq 1$. Thus the role of the $\mu^2(d)$ in the summation in the denominator of the right hand side of the above inequality is only to restrict this summation to square free integers $d$.

We will obtain a proof of this theorem in two stages. The first is called the arithmetic part of the large sieve and the second the analytic part.

### 1. The Arithmetical Part of the Large Sieve.

The point of view here is to apply the fourier transform on $\mathbf{R}/\mathbf{Z}$ and its finite subgroups groups to study the question posed above. Recall that $\mathbf{Z}$ is identified with the dual group of $\mathbf{R}/\mathbf{Z}$, which we shall hereafter denote by $\mathbf{T}$, by means of the map $n \mapsto e^{2\pi i n t}$. In particular, for any subset $X$ of $\mathbf{Z}$ this identification allows us to write $\chi \in X$ for the set of characters $e^{2\pi i n t}$ with $n \in X$. With this identification we now consider trignometric polynomials supported in $A$, that is, trignometric polynomials of the form

$$f(t) \;=\; \sum_{\chi\in A} a_\chi \chi(t) \,, \tag{10}$$

where $a_\chi$ are arbitrary complex numbers.

1.1 Let $\mathbf{T}_d$ for any integer $d \geq 1$ denote the $d$ torsion subgroup of $\mathbf{T}$. This is, by definition, the subgroup of $\mathbf{T}$ comprising the elements $x$ of $\mathbf{T}$ satisfying the relation $dx = 0$. Check that $\mathbf{T}_d$ is a cyclic group of order $d$.

1.2 The characters of $\mathbf{T}$ when restricted to $\mathbf{T}_d$ are characters for this group. Check that $e^{2\pi int}$ and $e^{2\pi imt}$ define the same character of $\mathbf{T}_d$ if and only if $n$ and $m$ are the same modulo $d$. Conclude we may identify $\mathbf{Z}/d\mathbf{Z}$ with the dual group of $\mathbf{T}_d$ by the that associates the class of an integer $k$ modulo $d$ with $e^{2\pi ikt}$.

With the identification of $\mathbf{Z}/d\mathbf{Z}$ with the dual group of $\mathbf{T}_d$ given above, subsets of $\mathbf{Z}/d\mathbf{Z}$ are indentified with sets of characters of $\mathbf{T}_d$.

1.3 Let $p$ be a prime number. Check that for any $\chi$ in $\hat{\mathbf{T}}_p$ we have $\chi \notin A_p \implies \hat{f}(\chi) = 0$ where $f$ is the restriction of the trignometric polynomial $f$ of the form (10) to $\mathbf{T}_p$. Now justify the following relations.

$$|f(0)|^2 = |\sum_{\chi \in A_p} \hat{f}(\chi)| \leq |A_p| \sum_{\chi \in \mathbf{Z}/p\mathbf{Z}} |\hat{f}(\chi)|^2 = v_p \sum_{x \in \mathbf{T}_p} |f(x)|^2 \tag{11}$$

Conclude from the above relations that for any prime number $p$ and any trignometric polynomial of the form (10) we have

$$|f(0)|^2 \left(\frac{1 - v_p}{v_p}\right) \leq \sum_{\substack{x \in \mathbf{T}_p, \\ x \neq 0}} |f(x)|^2 = \sum_{\substack{x \in \mathbf{T}, \\ \mathrm{ord}(x) = p}} |f(x)|^2 . \tag{12}$$

1.5 Suppose that $d$ is a square-free integer. Then using (13) and induction on the number of prime divisors of $d$ deduce that

$$|f(0)|^2 \prod_{p|d} \left(\frac{1 - v_p}{v_p}\right) \leq \sum_{\substack{x \in \mathbf{T}, \\ \mathrm{ord}(x) = d}} |f(x)|^2 . \tag{13}$$

*Hint.*— Suppose that $d = p_1 p_2$, that is, $d$ has two primefactors. Then obtain the relations

$$\sum_{\substack{x \in \mathbf{T}, \\ \mathrm{ord}(x) = d}} |f(x)|^2 = \sum_{\substack{x_1 \in \mathbf{T}, \\ \mathrm{ord}(x_1) = p_1}} \sum_{\substack{x_2 \in \mathbf{T}, \\ \mathrm{ord}(x_2) = p_2}} |f(x_1 + x_2)|^2 \geq \left(\frac{1 - v_{p_1}}{v_{p_1}}\right) \sum_{\substack{x_1 \in \mathbf{T}, \\ \mathrm{ord}(x_1) = p_1}} |f(x_1)|^2 . \tag{14}$$

To obtain the first relation note that by the chinese remainder theorem every $x \in \mathbf{T}$ can be written in a unique manner as $x_1 + x_2$, where $x_1$ and $x_2$ are elements of $\mathbf{T}$ of orders $p_1$ and $p_2$

respectively. The second relation is deduced by applying, for each $x_1$, (12) to the trignometric polynomial $f(x_1 + x)$ which is also of the form (10). Now apply (12) again but this time to $f(x)$ itself to obtain (13) when $d = p_1 p_2$.

1.6 Conclude that for any trignometric polynomial of the form (10) and integer $Q \geq 1$ we have the inequality

$$|f(0)|^2 \sum_{1 \leq d \leq Q} \mu^2(d) \prod_{p|d} \left( \frac{1 - v_p}{v_p} \right) \leq \sum_{\substack{x \in \mathbf{T}, \\ 1 \leq \mathrm{ord}(x) \leq Q}} |f(x)|^2 \, . \tag{15}$$

What is $f(0)$ when all the $a_\chi$ are taken to be 1 ?

**2. The Analytic Large Sieve Inequality**

In this section we will obtain the inequality

$$\sum_{\substack{x \in \mathbf{T}, \\ 1 \leq \mathrm{ord}(x) \leq Q}} |f(x)|^2 \leq (N - 1 + Q^2) \sum_{\chi \in A} |a_\chi|^2 \, . \tag{16}$$

for all trignometric polynomials $f$ of the form (10)

For any $x$ in $\mathbf{T} = \mathbf{R}/\mathbf{Z}$, we set $\|x\| = \inf_{n \in \mathbf{Z}} |x - n|$. For a $\delta > 0$, we say that a set of points $x_1, x_2, \ldots, x_l$ of $\mathbf{T}$ is a $\delta$-spaced if $\|x_i - x_j\| \geq \delta$ for any distinct $i$ and $j$.

2.1 Check that the set of $x$ in $\mathbf{T}$ with $1 \leq \mathrm{ord}(x) \leq Q$ is the same as the union of the $\mathbf{T}_d$ with $1 \leq d \leq Q$ and that this union is a $\frac{1}{Q^2}$ spaced subset of $\mathbf{T}$.

2.2 Verify using the duality principle that in order to obtain (16) it suffices to show that for any $\delta$-spaced set $x_1, x_2, \ldots, x_l$ of points on $\mathbf{T}$ and any complex numbers $b_1, b_2, \ldots, b_l$ we have

$$\sum_{M+1 \leq n \leq M+N} |\sum_{1 \leq i \leq l} b_i e^{2\pi i n x_i}|^2 \leq \left( N - 1 + \frac{1}{\delta} \right) \sum_{1 \leq i \leq l} |b_i|^2 \, . \tag{17}$$

2.3 Let $I = [M + 1, M + N]$ and $\phi$ be the Selberg-Beurling function contructed earlier. With $b_i$ and $x_i$ as above justify the relations

$$\sum_{M+1 \leq n \leq M+N} |\sum_{1 \leq i \leq l} b_i e^{2\pi i n x_i}|^2 \leq \sum_{n \in \mathbf{Z}} \phi(n) |\sum_{1 \leq i \leq l} b_i e^{2\pi i n x_i}|^2 = \sum_{1 \leq i,j \leq} b_i \overline{b_j} \sum_{n \in \mathbf{Z}} \hat{\phi}(x_i - x_j + n) \, . \tag{18}$$

Noting that $x_i$ are $\delta$-spaced deduce (18).

2.4 Combine the preceding parts to conclude the Theorem stated at the head of this part (the large sieve).

## Applications

We obtain two simple applications of the large sieve.

3.1 Suppose $A$ is a subset of $[M+1, M+N]$ such that $v_p$ may be taken as $\alpha$ for all prime numbers upto $N^{1/2}$. Applying the large sieve with $Q = N^{1/2}$ show that $|A| \ll N^{1/2} \log N$. This means that if a set integers in $[M+1, M+N]$ misses a fixed proportion of residue classes modulo $p$ for all primes $p$ upto $N^{1/2}$ then the cardinality of the set must be very small !

3.2 Show that for any $M \geq N \geq 1$ the number of prime numbers in the interval $[M+1, M+N]$ is $\ll N/\log N$. To do this apply (with justification) the large sieve with $Q = N^{1/2}$ and $A_p$ taken to be the invertible residue classes in $\mathbf{Z}/p\mathbf{Z}$ for each prime $p \leq N^{1/2}$. Finally, note the following inequalities

$$\sum_{1 \leq d \leq Q} \mu^2(d) \prod_{p|d} \frac{1}{p-1} \;=\; \sum_{1 \leq d \leq Q} \frac{\mu^2(d)}{\phi(d)} \;\geq\; \sum_{1 \leq d \leq Q} \frac{1}{d} \;\gg\; \log Q \; . \tag{19}$$