Dirichlet Theorem

Harsh Kumar
Roll : 12284
MTH 391
Mentor: Shobha Madan

November 6, 2014

1 Introduction

The aim of the project is to understand the proof of the famous Dirichlet's theorem on arithmetic progressions.

Theorem 1.1 (Dirichlet, 1837). *Let $a, N \in \mathbb{Z}^+$ be such that $gcd(a, N) = 1$. Then, there are infinitely many prime in the arithmetic progression $a, a + N, a + 2N, a + 3N, \ldots, a + kN, \ldots$*

Here we have presented all the results studied during the course of the project. The detailed proofs can found in [1].

2 Notation

We have used standard mathematical notations through out the text. Also, most of the notations have been defined before usage. But a note is due for the asymptotic notation used in the text. The big O notation is

$$f(x) = O(g(x))$$

if for some constant c,

$$|f(x)| \leq c|g(x)|.$$

Also, by $\mathbb{Z}^*(q)$ we mean the set of positive integers less than q that are relatively prime to q. It is easy to see that this set forms a group under multiplication.

3 Finite Fourier Analysis

The project began with the study of Fourier analysis on finite abelian groups. Let G be a finite abelian group and S^1 be the unit circle in the complex plane.

Definition 3.1. *A character on G is a complex-valued function $e : G \longmapsto S^1$ such that $e(ab) = e(a)e(b) \quad$ for all $a, b \in G$*

Hence characters of a group are by definition multiplicative. The trivial or unit character is defined by $e(a) = 1$ for all $a \in G$. We denote the set of all characters of G by $\hat{G}$. We note that this set forms an abelian group under multiplication defined by $(e_1.e_2)(a) = e_1(a)e_2(a)$ for all $a \in G$ and the trivial character acting as the unit of this group. This group is called the dual group of G.

Lemma 3.2. *Let $e : G \to \mathbb{C} \setminus \{0\}$ a multiplicative function, that is $e(a.b) = e(a)e(b)$ for all $a, b \in G$. Then e is a character.*

Proof. As the group G is finite $|e(a)|$ is bounded both above and below. Now as $|e(b^n)| = |e(b)|^n$ and $e(a) \neq 0$, so $|e(b)| = 1$ for all $b \in G$. Hence e is a character of G. □

Note that if e is a non-trivial character of the group G, then $\sum_{a \in G} e(a) = 0$. As we can choose a $b \in G$ such that $e(b) \neq 1$. And

$$e(b) \sum_{a \in G} e(a) = \sum_{a \in G} e(b)e(a) = \sum_{a \in G} e(ab) = \sum_{a \in G} e(a)$$

So, $\sum_{a \in G} e(a) = 0$.

Now, let V be the vector space of complex-valued functions defined on G. We define a Hermitian inner product on V by

$$< f, g >= \frac{1}{|G|} \sum_{a \in G} f(a)\overline{g(a)}$$

where $f, g \in V$.

Theorem 3.3. *The characters of G form an orthogonal family with respect to this inner product.*

Theorem 3.4. *The characters of G form an orthogonal basis for the vector space of complex-valued functions on G.*

The proof of this theorem involved an extension of the spectral theorem

Theorem 3.5 (Spectral Theorem). *Every normal linear transformation on a finite dimensional vector space can be diagonalized.*

proof of this theorem can be found in [2]

Definition 3.6 (Fourier coefficient). *The Fourier coefficient of a function f with respect to a character e is given by*

$$\hat{f}(e) = \frac{1}{|G|} \sum_{a \in G} f(a)\overline{g(a)}$$

Theorem 3.7. *The characters of G form an orthogonal basis for the vector space V of function on G equipped with the inner product*

$$< f, g >= \frac{1}{|G|} \sum_{a \in G} f(a)\overline{g(a)}$$

Also, any function f on G equals its Fourier series

$$f = \sum_{e \in \hat{G}} \hat{f}(e)e$$

where $\hat{G}$ is the set of all characters on G

Also, this gives us the Parseval-Plancherel formula for finite abelian groups

$$\|f\|^2 = \sum_{e \in \hat{G}} \left|\hat{f}(e)\right|^2$$

4 Zeta function

We define the zeta function by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Theorem 4.1 (Euler's product formula). *For all $s > 1$,*

$$\zeta(s) = \prod_p \frac{1}{1 - p^{-s}}$$

where the product is over the set of all primes.

This theorem can be proved using the fundamental theorem of arithmetic. Also, note that

$$\zeta(s) \leq 1 + \frac{1}{s-1}$$

.

5 Dirichlet's Theorem

Now we return to the main aim of this project : to prove the Drichlet's Theorem. To this end we will try to simplify the problem by introducing the concept of Dirichlet characters.

5.1 Dirichlet characters

Let us call G to be the abelian group $\mathbb{Z}^*(q)$. Clearly, $|G| = \varphi(q)$ where $\varphi(q)$ is the Euler phi-function (the number of integers $0 \leq n < q$ that are reltively prime to q).

Let $\hat{G}$ be the set of characters of G. So using these we can write fourier series of any function from G to $\mathbb{C}$. Now, consider the function δ_l (the characteristic function of l in G).

$$\delta_l(n) = \begin{cases} 1 & \text{if } n \equiv l \mod q \\ 0 & \text{otherwise} \end{cases}$$

So, for any $n \in G$,

$$\delta_l(n) = \sum_{e \in \hat{G}} \hat{\delta}_l(e) e(n)$$

where, $\hat{\delta}_l = \frac{1}{|G|} \sum_{m \in G} \delta_l(m) \overline{e(m)} = \frac{1}{|G|} \overline{e(l)}$. So,

$$\delta_l(n) = \frac{1}{|G|} \sum_{e \in \hat{G}} \overline{e(l)} e(n)$$

We extend the characters $e \in \hat{G}$ to all of $\mathbb{Z}$ as follows:

$$\chi(m) = \begin{cases} e([m]), & \text{if } m, q \text{ are reletively prime} \\ 0, & \text{otherwise} \end{cases}$$

where $[m]$ is the number $l \in \{1, 2, \ldots, q\}$ such that $m \pmod q = l \pmod q$. These χ are called the Dirichlet characters modulo q. The trivial dirichlet character is the extension of the trivial character.

Lemma 5.1. *The Dirichlet characters are multiplicative. Additionally, for all $n \in \mathbb{Z}$*

$$\delta_l(n) = \frac{1}{|G|} \sum_{e \in \hat{G}} \overline{\chi(l)} \chi(n)$$

The multiplicity is a direct consequence of the multiplicity of characters e and we get the equation by extending δ_l to all of $\mathbb{Z}$.

Lemma 5.2. *If χ is a non-trivial Drichlet character, then*

$$|\sum_{n=1}^{k}\chi(n)| \leq q, \qquad \textit{for any } k$$

Proof. Let $\sum_{n=1}^{q}\chi(n) = S$ then, for all $a \in G$

$$\chi(a)S = \sum \chi(a)\chi(n) = \sum \chi(an) = \sum \chi(n) = S$$

Now, as χ is non-trivial, there exists a $a \in G$ such that $\chi(a) \neq 1$, hence $S = 0$.

Now write any $k \in \mathbb{Z}$ as $aq + b$ where $0 \leq b < q$, then

$$\begin{aligned}
|\sum_{n=1}^{k}\chi(n)| &= |\sum_{n=1}^{aq}\chi(n) + \sum_{n=aq+1}^{aq+b}\chi(n)| \\
&= |\sum_{n=aq+1}^{aq+b}\chi(n)| \\
&\leq \sum_{n=aq+1}^{aq+b}|\chi(n)| \\
&\leq b && \text{as } |\chi(n)| \leq 1 \\
&\leq q
\end{aligned}$$

□

Note that these are the only two properties of the Dirichlet characters used to prove to the theorem.

5.2 Dirichlet L-functions

We define the L-function as follows :

$$L(s,\chi) = \sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}$$

This is well defined for for $s > 1$.

Proposition 5.3. *If χ_0 is the trivial Dirichlet character and $q = p_1^{a_1}\ldots p_N^{a_N}$ is the prime factorization of q. Then,*

$$L(s,\chi_0) = (1 - p_1^{-s})(1 - p_2^{-s})\ldots(1 - p_N^{-s})\zeta(s)$$

And so $L(s,\chi)$ tends to ∞ as s tends to 1^+. Additionally, $L(s,\chi_0) = O(1/|s-1|)$ as $s \to 1$.

Proposition 5.4. *If χ is a non-trivial character, then*

$$\sum_{n=1}^{\infty} \chi(n)/n^s$$

converges for $s > 0$ and we denote this sum by $L(s,\chi)$. Also, $L(s,\chi)$ is continuously differentiable for $0 < s < \infty$.

Theorem 5.5. *If $s > 1$, then*

$$\sum_{n=1}^{\infty} = \prod_{p} \frac{1}{1-\chi(p)p^{-s}}$$

where the product is over all primes.

Now we define two logarithm functions.
For $z \in \mathbb{C}$ with $|z| < 1$,

$$\log_1(\frac{1}{1-z}) = \sum_{k=1}^{\infty} \frac{z^k}{k}$$

We can show that $e^{\log_1(\frac{1}{1-z})} = \frac{1}{1-z}$.Additionally, Also, if $|z| < 1$ then

$$|\log_1(\frac{1}{1-z})| \leq 2|z|$$

This also implies the convergence of $\prod_{n=1}^{\infty} \frac{1}{1-a_n}$ and that the product is non-zero.

Now we define the logrithm for $L(s,\chi)$ as(for non-trivial Dirichlet character) :

$$\log_2 L(s,\chi) = -\int_s^{\infty} \frac{L'(t,\chi)}{l(t,\chi)} dt$$

Again we can prove that $e^{\log_2 L(s,\chi)} = L(s,\chi)$.

These function $\log_1$ and $\log_2$ are related by the following relation:

$$\log_2 L(s,\chi) = \sum_{p} \log_1(\frac{1}{1-\chi(p)p^{-s}}),$$

that is they are the same branch of logarithm in the complex plane. This implies that (for non-trivial Dirichlet character)

$$\begin{aligned}\log_2 L(s,\chi) &= \sum_p \frac{\chi(p)}{p^s} + O(\sum_p \frac{1}{p^{2s}}) \\ &= \sum_p \frac{\chi(p)}{p^s} + O(1)\end{aligned}$$

So,$\sum_p \frac{\chi(p)}{p^s}$ would be bounded if $L(s,\chi)$ is not equal to 0. Using all these results and some additional inequalities of the Dirichlet character, we can prove that if $\chi \neq \chi_0$, then $L(1,\chi) \neq 0$.

5.3 $L(1,\chi) \neq 0$

For the complex case
The case when χ is a complex function.

Lemma 5.6.

$$\prod_\chi L(s,\chi) \geq 1$$

where the product is over all characters.

This can be proved by using $L(s,\chi) = \exp(\sum_p \log_1(\frac{1}{1-\chi(p)p^{-s}}))$.

Lemma 5.7. *If* $L(1,\chi) = 0$ *then* $L(1,\overline{\chi}) = 0$*.*

This is because $L(1,\overline{\chi}) = \overline{L(1,\chi)} = 0$.

Lemma 5.8. *If* χ *is non-trivial and* $L(1,\chi) = 0$ *then* $|L(s,\chi)| = O(s-1)$ *as* $s \to 1$*.*

This can be obtained by applying mean value theorem to $L(s,\chi)$ with respect to the variable s.

Now assume $L(1,\chi') = 0$ where χ' is complex then

$$\prod_{\chi]} L(s,\chi) = L(s,\chi_0)L(s,\chi')L(s,\overline{\chi'}) \prod_{\text{other } \chi} L(s,\chi)$$

Now, $|L(s,\chi')| = O(s-1)$ and $|L(s,\overline{\chi'})| = O(s-1)$ and $|L(s,\chi_0)| = O(\frac{1}{s-1})$. So, the RHS tends to 0 as $s \to 1^+$, but we know that the LHS is greater than 1. Hence we have reached a contradiction. This implies that $L(1,\chi') \neq 0$ if χ' is complex.

For the real case

The case when χ is a real function. This part is slightly more complex.

We first take note of the following inequalities:

$$\sum_{n=1}^{N} \frac{1}{n} = \log N + O(1)$$

$$\sum_{n=1}^{N} \frac{1}{n^{1/2}} = \int_{1}^{N} +O(1)$$

These can be obtained by comparing these summations with their respective integrals. Additionally we can also prove the following inequalities :

$$\sum_{n=1}^{N} \frac{\chi(n)}{n^{1/2}} = O(a^{-1/2})$$

$$\sum_{n=1}^{N} \frac{\chi(n)}{n} = O(a^{-1})$$

These can be proved by substituting $s_n - s_{n-1}$ in place of $\chi(n)$, where $s_n = \sum_{k=1}^{n} \chi(k)$.

Now we define

$$F(m.n) = \frac{\chi(n)}{(nm)^{1/2}}.$$

Also, let

$$S_N = \sum \sum_{mn \leq N} F(m, n)$$

where m, n are positive integers.

Lemma 5.9.

$$\sum_{n|k} \chi(n) \geq \begin{cases} 0 & \textit{for all } k \\ 1 & \textit{if } k = l^2 \textit{for some } l \in \mathbb{Z}. \end{cases}$$

So we get

$$S_N \geq \sum_{k=l^2,\ l \leq N^{1/2}} \frac{1}{n^{1/2}} = O(\log N^{1/2}) = O(\log N).$$

Now using the technique of hyperbolic sums we can also prove that $S_N = 2N^{1/2}L(1, \chi) + O(1)$. But $S_N = O(\log N)$, so $L(1, \chi)$ cannot be 0 if χ is real.

5.4 Proof of Dirichlet Theorem

The aim is to prove that

$$\sum_{p \equiv l \mod q} \frac{1}{p}$$

diverges as this implies that there a infinite primes p of the form $p \equiv l \mod q$. This obviously requires l and q to be relatively prime.

The above aim can be restated as proving that $\sum_{p\equiv l \mod q} \frac{1}{p^s}$ tends to ∞ as s tends to 1^+.

Now we can write this summation using the δ_l function as

$$\begin{aligned}
\sum_{p \equiv l \mod q} \frac{1}{p^s} &= \sum_{p \equiv l \mod q} \frac{\delta_l}{p^s} \\
&= \frac{1}{\varphi(q)} \sum_{p} \frac{\chi_0(p)}{p^s} + \frac{1}{\varphi(q)} \sum_{\chi \neq \chi_0} \overline{\chi(l)} \sum_{p} \frac{\chi(p)}{p^s} \\
&= \frac{1}{\varphi(q)} \sum_{p \nmid q} \frac{1}{p^s} + \frac{1}{\varphi(q)} \sum_{\chi \neq \chi_0} \overline{\chi(l)} \sum_{p} \frac{\chi(p)}{p^s}
\end{aligned}$$

where summations are over primes.

Now on the RHS the first term diverges as $s \to 1^+$ but the second part converges as there are finite Dirichlet characters for a given q and each of the inner summation converges as $s \to 1^+$. Hence the RHS diverges as $s \to 1^+$.

References

[1] Elias M . Stein, Rami Shakarchi(2003) *Fourier Analysis: An Introduction Volume 1 of Princeton lectures in analysis*(2nd edition), New Jersey: Princeton University Press, pp 218-275

[2] George F. Simmons(2004) *Introduction To Topology And Modern Analysis*, New Delhi: Tata MaGraw-Hill Publishing