L-function and the theorem on arithmetic progressions

Kangsig Kim

April 19, 2019

Abstract. We define the Dirichlet L-function and use its properties to prove that there exist infinitely many prime numbers p such that $p \equiv a \pmod{m}$ where a and m are relatively prime integers ≥ 1.

1 Dirichlet series

Let (λ_n) be an increasing sequence of real numbers tending to infinity. A *Dirichlet series* with exponents (λ_n) is a series of the form

$$f(z) = \sum_{n=1}^{\infty} a_n e^{-\lambda_n z} \quad (a_n \in \mathbb{C}, z \in \mathbb{C})$$

These are the properties of Dirichlet series which can be proved by using the theories of complex analysis.

Proposition 1. If f converges for $z = z_0$, it converges for $\Re(z) > \Re(z_0)$ and it is holomorphic in that domain.

Proposition 2. Let a_n are real ≥ 0. Suppose that f converges for $\Re(z) > \rho$ and that f can be extended analytically to a function holomorphic in a neighborhood of the point $z = \rho$. Then there exists $\epsilon > 0$ such that f converges for $\Re(z) > \rho - \epsilon$.

When $\lambda_n = \log n$, we get $f(s) = \displaystyle\sum_{n=1}^{\infty} \frac{a_n}{n^s}$, which is a form of the zeta function and L-function. The notation s being traditional for the variable.

Proposition 3. If a_n are bounded, then $f(s) = \displaystyle\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ converges absolutely for $\Re(s) > 1$.

This follows from the convergence of $\displaystyle\sum_{n=1}^{\infty} \frac{1}{n^{\alpha}}$ for $\alpha > 1$, $\alpha \in \mathbb{R}$

Proposition 4. If every partial sum $\displaystyle\sum_{n=m}^{n=p} a_n$ is bounded, then $f(s) = \displaystyle\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ converges (not necessarily absolute) for $\Re(s) > 0$.

2 Zeta function

In the following, P denotes the set of prime numbers. Recall the properties of the zeta function $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in P} \frac{1}{1-p^{-s}}$, which equalities holds for $\Re(s) > 1$.

Proposition 5. (a) $\zeta(s)$ is holomorphic and nonzero for $\Re(s) > 1$.
(b) $\zeta(s) = \frac{1}{s-1} + \phi(s)$, where $\phi(s)$ is holomorphic for $\Re(s) > 0$. Thus $\zeta(s)$ extends analytically for $\Re(s) > 0$ and has a simple pole at $s = 1$.

Proposition 6. When $s \to 1$, one has $\sum_{p \in P} p^{-s} \sim \log\ 1/(s-1)$, and $\sum_{p \in P, k \geq 2} 1/p^{ks}$ remains bounded.

Proof) Using that $\log(1-z) = -(z + \frac{z^2}{2} + \frac{z^3}{3} + \ldots)$ for $|z| < 1$, one has:

$$\log \zeta(s) = \log \prod_{p \in P} \frac{1}{1-p^{-s}} = \sum_{p \in P} -\log(1-p^{-s}) = \sum_{p \in P,\ k \geq 1} \frac{1}{k \cdot p^{ks}} = \sum_{p \in P} 1/p^s + \psi(s)$$

where $\psi(s) = \sum_{p \in P,\ k \geq 2} (1/k \cdot p^{ks})$. The series $\psi(s)$ is majorized by

$$\sum_{p \in P,\ k \geq 2} 1/p^{ks} = \sum 1/p^s(p^s - 1) \geq \sum 1/p(p-1) \geq \sum_{n=2}^{\infty} 1/n(n-1) = 1.$$

Thus $\psi(s)$ is bounded, and since proposition 5(b) shows that $\log \zeta(s) \sim \log\ 1/(s-1)$ as $s \to 1$, we get $\sum_{p \in P} p^{-s} \sim \log\ 1/(s-1)$.

3 Characters of finite abelian groups and L-functions

Let G be a finite abelian group. A *character* of G is a homomorphism of G into the multiplicative group $\mathbb{C}^*$ of complex numbers. The characters of G form a group $Hom(G, \mathbb{C}^*)$ which we denote by $\hat{G}$ and call the *dual* of G. Note that the group $\hat{G}$ is also a finite abelian group of the same order as G. For $\chi \in \hat{G}$ and $x \in G$, we have $|\chi(x)| = 1$ because $\chi(x)^n = \chi(x^n) = \chi(1) = 1$ where n is the order of x.

Proposition 7. Let n be the order of G and let $\chi \in \hat{G}$. Then

$$\sum_{x \in G} \chi(x) = \begin{cases} n, & if\ \chi = 1 \\ 0, & if\ \chi \neq 1 \end{cases}$$

Proof) The first formula is obvious. To prove the second, choose $y \in G$ such that $\chi(y) \neq 1$. Then $\chi(y) \sum_{x \in G} \chi(x) = \sum_{x \in G} \chi(xy) = \sum_{x \in G} \chi(x)$, hence $(\chi(y) - 1) \sum_{x \in G} \chi(x) = 0$. Since $\chi(y) \neq 1$, this implies $\sum_{x \in G} \chi(x) = 0$.

Proposition 8. Let $x \in G$. Then

$$\sum_{\chi \in \hat{G}} \chi(x) = \begin{cases} n, & if\ x = 1 \\ 0, & if\ x \neq 1. \end{cases}$$

This follows from Proposition 7 applied to the dual group $\hat{G}$.

Let $m \geq 1$ be an integer. We let $(\mathbb{Z}/m\mathbb{Z})^*$ the multiplicative group of invertible elements of the ring $\mathbb{Z}/m\mathbb{Z}$ and let χ be a character of $(\mathbb{Z}/m\mathbb{Z})^*$. We can view χ as a multiplication function, defined on the set of integers prime to m, with values in $\mathbb{C}$. We extend the domain of the function to whole $\mathbb{Z}$ by putting $\chi(a) = 0$ if a is not prime to m.

The corresponding *L-function* is defined by the Dirichlet series

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

Proposition 9. For $\chi = 1$, we have $L(s, 1) = F(s)\zeta(s)$ with $F(s) = \prod_{p|m}(1 - p^{-s})$. In particular $L(s, 1)$ extends analytically for $\Re(s) > 0$ and has a simple pole at $s = 1$.

Proposition 10. For $\chi \neq 1$, the series $L(s, \chi)$ converges in $\Re(s) > 0$ and converges absolutely in $\Re(s) > 1$; one has

$$L(s, \chi) = \prod_{p \in P} \frac{1}{1 - \chi(p)p^{-s}} \quad for \quad \Re(s) > 1$$

Proof) The assertion for absolute convergence in $\Re(s) > 1$ follows from proposition 3. Thus in $\Re(s) > 1$, we get a series of equalities

$$L(s, \chi) = \sum_{n=1}^{\infty} \chi(n)/n^s = \prod_{p \in P} \left(\sum_{m=0}^{\infty} \chi(p^m)/p^{ms} \right) = \prod_{p \in P} \frac{1}{1 - \chi(p)p^{-s}}$$

. Here, we used that $\chi(ab) = \chi(a)\chi(b)$ for every $a, b \in \mathbb{Z}$. It remains to show the convergence of $L(s, \chi)$ for $\Re(s) > 0$. Using proposition 4, it suffices to show that $\sum_{n=u}^{n=v} \chi(n)$ are bounded. By proposition 7, we have $\sum_{n=u}^{n=u+m-1} \chi(n) = 0$. Thus it suffices to majorize $\sum_{n=u}^{n=v} \chi(n)$ for $v - u < m - 1$. But since $|\chi(x)| = 1$, one has $|\sum_{n=u}^{n=v} \chi(n)| \leq \phi(m)$ where $\phi(m)$ is an order of the group $(\mathbb{Z}/m\mathbb{Z})^*$, given by the Euler ϕ-function of m. This completes the proof.

4 The theorem of non-vanishing L-functions

The key point of Dirichlet's proof is to show that $L(1,\chi) \neq 0$ for all $\chi \neq 1$. To show it, we introduce the product of the L-functions relative to the same integer m.

Let $m \geq 1$ be an integer. If prime number p does not divide m, we let $f(p)$ the order of p in $(\mathbb{Z}/m\mathbb{Z})^*$. That is, $f(p)$ is the smallest integer $f > 1$ such that $p^f \equiv 1 \pmod{m}$. We put $g(p) = \phi(m)/f(p)$.

Lemma 1. If $p \nmid m$, then $\prod_{\chi}(1-\chi(p)T) = (1-T^{f(p)})^{g(p)}$, where the product extends over all characters χ of $(\mathbb{Z}/m\mathbb{Z})^*$.

Proof) Let W be the set of $f(p)$-th roots of unity. Then

$$\begin{aligned}
T^{f(p)} - 1 &= \prod_{w\in W}(T-w) = (-1)^{f(p)}\prod_{w\in W}(w-T) \\
&= (-1)^{f(p)}\Big(\prod_{w\in W} w\Big)\Big(\prod_{w\in W}(1-w^{-1}T\Big) = -\prod_{w\in W}(1-w^{-1}T) = -\prod_{w\in W}(1-wT),
\end{aligned}$$

so we get $\prod_{w\in W}(1-wT) = 1-T^{f(p)}$. Now for each $w \in W$ there exists $g(p)$ characters χ of $(\mathbb{Z}/m\mathbb{Z})^*$ such that $\chi(p) = w$. Hence $\prod_{\chi}(1-\chi(p)T) = (1-T^{f(p)})^{g(p)}$ holds.

We define a function $\zeta_m(s)$ by

$$\zeta_m(s) = \prod_{\chi} L(s,\chi),$$

where the product extends over all characters χ of $(\mathbb{Z}/m\mathbb{Z})^*$.

Proposition 11. One has

$$\zeta_m(s) = \prod_{p\nmid m}\frac{1}{(1-p^{-f(p)s})^{g(p)}}.$$

This is a Dirichlet series, with positive integral coefficients, converging in $\Re(s) > 1$.

Proof) Replacing each L-function by its product expansion, and applying lemma 1 (with $T = p^{-s}$) noticing that $\chi(p) = 0$ if p divides m, we obtain the product expansion of $\zeta_m(s)$. The assertion for convergence in $\Re(s) > 1$ follows from proposition 9, 10 and the equality $\zeta_m(s) = \prod_{\chi} L(s,\chi)$. And since

$$\zeta_m(s) = \prod_{p\nmid m}\frac{1}{(1-p^{-f(p)s})^{g(p)}} = \prod_{p\nmid m}(1+\frac{1}{p^{f(p)s}}+\frac{1}{p^{2f(p)s}}+\frac{1}{p^{3f(p)s}}+\ldots)^{g(p)} \quad for \quad \Re(s) > 1,$$

we deduce that $\zeta_m(s)$ is a Dirichlet series with positive integral coefficients.

Theorem 1. *$L(1,\chi) \neq 0$ for all $\chi \neq 1$.*

Proof) Suppose that $L(1,\chi) = 0$ for some $\chi \neq 1$. Then $\zeta_m(s)$ would be holomorphic at $s = 1$, thus also for all s in $\Re(s) > 0$ by proposition 9, 10. Since $\zeta_m(s)$ is a Dirichlet series with positive coefficients, it would converge for all s in the same domain by proposition 2. (take ρ be very small positive real number in proposition 2)
However, the p-th factor of $\zeta_m(s)$ is

$$\frac{1}{(1-p^{-f(p)s})^{g(p)}} = (1 + p^{-f(p)s} + p^{-2f(p)s} + ...)^{g(p)}$$

and it dominates $1 + p^{-\phi(m)s} + p^{-2\phi(m)s} + ...$
It follows that $\zeta_m(s)$ dominates the series $\displaystyle\sum_{(n,m)=1} n^{-\phi(m)s}$ which diverges for $s = \frac{1}{\phi(m)}$.

It contradicts the convergence of $\zeta_m(s)$ in $\Re(s) > 0$. This completes the proof.

Define the series:

$$f_\chi(s) = \sum_{p \nmid m} \frac{\chi(p)}{p^s}$$

This series being convergent for $\Re(s) > 1$ by proposition 3. We get essential properties of $f_\chi(s)$ for $s \to 1$ by using theorem 1.

Proposition 12. If $\chi = 1$, then $f_\chi(s) \sim \log \frac{1}{s-1}$ for $s \to 1$

This follows from proposition 6 and the fact that f_1 differs from the series $\displaystyle\sum_{p \in P} \frac{1}{p^s}$ by a finite number of terms only.

Proposition 13. If $\chi \neq 1$, then $f_\chi(s)$ remains bounded when $s \to 1$.

Proof) Use again the identity $\log(1-z) = -(z + \frac{z^2}{2} + \frac{z^3}{3} + ...)$ for $|z| < 1$.
Then for $\Re(s) > 1$, one has:

$$\log L(s,\chi) = \sum_{p \nmid m} \log \frac{1}{1-\chi(p)p^{-s}} = \sum_{n \geq 1, p \nmid m} \frac{\chi(p)^n}{np^{ns}} = f_\chi(s) + F_\chi(s)$$

with $F_\chi(s) = \displaystyle\sum_{n \geq 2, p \nmid m} \frac{\chi(p)^n}{np^{ns}}$.

Theorem 1, proposition 6, 10 shows that $\log L(s,\chi)$ and $F_\chi(s)$ remain bounded when $s \to 1$. Hence the same holds for $f_\chi(s)$.

Now we ready to prove the theorem on arithmetic progressions.

5 Density and Dirichlet theorem

Recall that when s tends to 1 (let s being real > 1 to fix the ideas),
one has $\displaystyle\sum_{p\in P} \frac{1}{p^s} \sim \log \frac{1}{s-1}$. Let A be a subset of P. One says that A has for *density* a real number k when the ratio

$$\left(\sum_{p\in A} \frac{1}{p^s}\right) \Big/ \left(\log \frac{1}{s-1}\right)$$

tends to k when $s \to 1$. One then has $0 \leq k \leq 1$. The theorem on arithmetic progressions can be refined in the following way:

Theorem 2. Let $m \geq 1$ and a be an integer such that $(a, m) = 1$. Let P_a be the set of prime numbers such that $p \equiv a \pmod{m}$. The set P_a has density $1/\phi(m)$.
(In other words, the prime numbers are "equally distributed" between the different classes modulo m which are prime to m.)

Proof) Define the series

$$g_a(s) = \sum_{p\in P_a} 1/p^s$$

We claim that $g_a(s) = \frac{1}{\phi(m)} \displaystyle\sum_{\chi} \chi(a)^{-1} f_\chi(s)$, where the sum extends over all characters χ of $(\mathbb{Z}/m\mathbb{Z})^*$. Observe that $\displaystyle\sum_{\chi} \chi(a)^{-1} f_\chi(s) = \sum_{p\nmid m} \Big(\sum_{\chi} \chi(a^{-1})\chi(p)\Big)/p^s$
and $\chi(a^{-1})\chi(p) = \chi(a^{-1}p)$. By proposition 8, we have:

$$\sum_{\chi} \chi(a^{-1}p) = \begin{cases} \phi(m), & if \;\; a^{-1}p \equiv 1 \;(mod\; m) \\ 0, & otherwise. \end{cases}$$

Thus the claim is proved. Now, as s tends to 1, proposition 12 shows that $f_\chi(s) \sim \log \frac{1}{s-1}$ for $\chi = 1$, and proposition 13 shows that all other f_χ remain bounded. Put them in $g_a(s) = \frac{1}{\phi(m)} \displaystyle\sum_{\chi} \chi(a)^{-1} f_\chi(s)$, we get $g_a(s) \sim \frac{1}{\phi(m)} \log \frac{1}{s-1}$ and this means that the density of P_a is $\frac{1}{\phi(m)}$.

Theorem 3 (Dirichlet). There exist infinitely many prime numbers p such that $p \equiv a \pmod{m}$ where a and m are relatively prime integers ≥ 1.

Proof) This is a corollary of theorem 2. Since the density of P_a is $\frac{1}{\phi(m)}$ which is a positive real number, the set P_a is infinite. Indeed a finite set has density zero.

References

[1] J.-P.Serre, *A Course in Arithmetic*, Springer, 1973