21. Primes in arithmetic progressions

Dirichlet's theorem is a strengthening of Euclid's theorem that there are infinitely many primes p. Dirichlet's theorem allows us to add the condition that $p = a \bmod N$ for fixed a invertible modulo fixed N, and still be assured that there are infinitely-many primes meeting this condition.

The most intelligible proof of this result uses a bit of analysis, in addition to some interesting algebraic ideas. The analytic idea already arose with Euler's proof of the infinitude of primes, which we give below. New algebraic ideas due to Dirichlet allowed him to isolate primes in different congruence classes modulo N.

In particular, this issue is an opportunity to introduce the **dual group**, or **group of characters**, of a finite abelian group. This idea was one impetus to the development of a more abstract notion of *group*, and also of *group representations* studied by Schur and Frobenious.

---

1. *Euler's theorem and the zeta function*

To illustrate how to use special functions of the form

$$Z(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

called **Dirichlet series** to prove things about primes, we first give Euler's proof of the infinitude of primes. [1]

[1] Again, the 2000 year old elementary proof of the infinitude of primes, ascribed to *Euclid* perhaps because his texts survived, proceeds as follows. Suppose there were only finitely many primes altogether, $p_1, \ldots, p_n$. Then $N = 1 + p_1 \ldots p_n$ cannot be divisible by any p_i in the list, yet has *some* prime divisor, contradiction. This viewpoint

The simplest Dirichlet series is the **Euler-Riemann** zeta function [2]

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

This converges absolutely and (uniformly in compacta) for real $s > 1$. For *real* $s > 1$

$$\frac{1}{s-1} = \int_1^\infty \frac{dx}{x^s} \leq \zeta(s) \leq 1 + \int_1^\infty \frac{dx}{x^s} = 1 + \frac{1}{s-1}$$

This proves that

$$\lim_{s \longrightarrow 1^+} \zeta(s) = +\infty$$

The relevance of this to a study of primes is the **Euler product expansion** [3]

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

To prove that this holds, observe that

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \ldots\right)$$

by unique factorization into primes. [4] Summing the indicated geometric series gives

$$\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1 - \frac{1}{p^s}}$$

Since sums are more intuitive than products, take a logarithm

$$\log \zeta(s) = \sum_p -\log(1 - \frac{1}{p^s}) = \sum_p \left(\frac{1}{p^s} + \frac{1}{2p^{2s}} + \frac{1}{3p^{3s}} + \ldots\right)$$

by the usual expansion (for $|x| < 1$)

$$-\log(1-x) = x + \frac{x^2}{2} + \frac{x^3}{3} + \ldots$$

Taking a derivative in s gives

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{p \text{ prime},\ m \geq 1} \frac{\log p}{p^{ms}}$$

Note that, for each fixed $p > 1$,

$$\sum_{m \geq 1} \frac{\log p}{p^{ms}} = \frac{(\log p)\, p^{-s}}{1 - p^{-s}}$$

---

does not give much indication about how to make the argument more *quantitative*. Use of $\zeta(s)$ seems to be the way.

[2] Studied by many other people before and since.

[3] Valid only for $s > 1$.

[4] Manipulation of this infinite product of infinite sums is not completely trivial to justify.

converges absolutely for real $s > 0$.

Euler's argument for the infinitude of primes is that, if there were only finitely-many primes, then the right-hand side of

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{p \text{ prime}, m \geq 1} \frac{\log p}{p^{ms}}$$

would converge for real $s > 0$. However, we saw that $\zeta(s) \longrightarrow +\infty$ as s approaches 1 from the right. Thus, $\log \zeta(s) \longrightarrow +\infty$, and $\frac{d}{ds}(\log \zeta(s)) = \zeta'(s)/\zeta(s) \longrightarrow -\infty$ as $s \longrightarrow 1^+$. This contradicts the convergence of the sum over (supposedly finitely-many) primes. Thus, there must be infinitely many primes. ///

---

2. *Dirichlet's theorem*

In addition to Euler's observation (above) that the analytic behavior[5] of $\zeta(s)$ at $s = 1$ implied the existence of infinitely-many primes, Dirichlet found an algebraic device to focus attention on single congruence classes modulo N.

[2.0.1] **Theorem:** *(Dirichlet)* Fix an integer $N > 1$ and an integer a such that $\gcd(a, N) = 1$. Then there are infinitely many primes p with

$$p = a \bmod N$$

[2.0.2] **Remark:** If $\gcd(a, N) > 1$, then there is at most one prime p meeting the condition $p = a \bmod n$, since any such p would be divisible by the *gcd*. Thus, the necessity of the *gcd* condition is obvious. It is noteworthy that beyond this *obvious* condition there is nothing further needed.

[2.0.3] **Remark:** For $a = 1$, there is a simple purely algebraic argument using cyclotomic polynomials. For general a the most intelligible argument involves a little analysis.

Proof: A **Dirichlet character** modulo N is a group homomorphism

$$\chi : (\mathbb{Z}/N)^\times \longrightarrow \mathbb{C}^\times$$

extended by 0 to all of $\mathbb{Z}/n$, that is, by defining $\chi(a) = 0$ if a is not invertible modulo N. This extension-by-zero then allows us to compose χ with the reduction-mod-N map $\mathbb{Z} \longrightarrow \mathbb{Z}/N$ and also consider χ as a function on $\mathbb{Z}$. Even when extended by 0 the function χ is still *multiplicative* in the sense that

$$\chi(mn) = \chi(m) \cdot \chi(n)$$

where or not one of the values is 0. The **trivial** character χ_o modulo N is the character which takes only the value 1 (and 0).

The standard **cancellation trick** is that

$$\sum_{a \bmod N} \chi(a) = \begin{cases} \varphi(N) & (\text{for } \chi = \chi_o) \\ 0 & (\text{otherwise}) \end{cases}$$

where φ is Euler's totient function. The proof of this is easy, by changing variables, as follows. For $\chi = \chi_o$, all the values for a invertible mod N are 1, and the others are 0, yielding the indicated sum. For $\chi \neq \chi_o$,

---

[5] Euler's proof uses only very crude properties of $\zeta(s)$, and only of $\zeta(s)$ as a function of a *real*, rather than *complex*, variable. Given the status of complex number and complex analysis in Euler's time, this is not surprising. It is slightly more surprising that Dirichlet's original argument also was a real-variable argument, since by that time, a hundred years later, complex analysis was well-established. Still, until Riemann's memoir of 1858 there was little reason to believe that the behavior of $\zeta(s)$ off the real line was of any interest.

there is an *invertible* b mod N such that $\chi(b) \neq 1$ (and is not 0, either, since b is invertible). Then the map $a \longrightarrow a \cdot b$ is a *bijection* of $\mathbb{Z}/N$ to itself, so

$$\sum_{a \bmod N} \chi(a) = \sum_{a \bmod N} \chi(a \cdot b) = \sum_{a \bmod N} \chi(a) \cdot \chi(b) = \chi(b) \cdot \sum_{a \bmod N} \chi(a)$$

That is,

$$(1 - \chi(b)) \cdot \sum_{a \bmod N} \chi(a) = 0$$

Since $\chi(b) \neq 1$, it must be that $1 - \chi(b) \neq 0$, so the sum is 0, as claimed.

Dirichlet's *dual* trick is to sum over characters χ mod N evaluated at fixed a in $(\mathbb{Z}/N)^\times$. We claim that

$$\sum_\chi \chi(a) = \begin{cases} \varphi(N) & (\text{for } a = 1 \bmod N) \\ 0 & (\text{otherwise}) \end{cases}$$

We will prove this in the next section.

Granting that, we have also, for b invertible modulo N,

$$\sum_\chi \chi(a)\chi(b)^{-1} = \sum_\chi \chi(ab^{-1}) = \begin{cases} \varphi(N) & (\text{for } a = b \bmod N) \\ 0 & (\text{otherwise}) \end{cases}$$

Given a Dirichlet character χ modulo N, the corresponding **Dirichlet L-function** is

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

Since we have the multiplicative property $\chi(mn) = \chi(m)\chi(n)$, each such L-function has an **Euler product** expansion

$$L(s, \chi) = \prod_{p \text{ prime},\ p \not| N} \frac{1}{1 - \chi(p)\, p^{-s}}$$

This follows as it did for $\zeta(s)$, by

$$L(s, \chi) = \sum_{n \text{ with } \gcd(n,N)=1} \frac{\chi(n)}{n^s}$$

$$= \prod_{p \text{ prime},\ p \not| N} \left(1 + \chi(p)p^{-s} + \chi(p)^2\, p^{-2s} + \ldots\right) = \prod_{p \text{ prime},\ p \not| N} \frac{1}{1 - \chi(p)\, p^{-s}}$$

by summing geometric series. Taking a logarithmic derivative (as with zeta) gives

$$-\frac{L'(s, \chi)}{L(s, \chi)} = \sum_{p \not| N \text{ prime},\, m \geq 1} \frac{\log p}{\chi(p)^m\, p^{ms}} = \sum_{p \not| N \text{ prime}} \frac{\log p}{\chi(p)\, p^s} + \sum_{p \not| N \text{ prime},\, m \geq 2} \frac{\log p}{\chi(p)^m\, p^{ms}}$$

The second sum on the right will turn out to be subordinate to the first, so we aim our attention at the first sum, where $m = 1$.

To pick out the primes p with $p = a$ mod N, use the sum-over-χ trick to obtain

$$\sum_{\chi \bmod N} \chi(a) \cdot \frac{\log p}{\chi(p)\, p^s} = \begin{cases} \varphi(N) \cdot (\log p)\, p^{-s} & (\text{for } p = a \bmod N) \\ 0 & (\text{otherwise}) \end{cases}$$

Thus,

$$- \sum_{\chi \bmod N} \chi(a) \frac{L'(s,\chi)}{L(s,\chi)} = \sum_{\chi \bmod N} \chi(a) \sum_{p \not| N \text{ prime}, m \geq 1} \frac{\log p}{\chi(p)^m \, p^{ms}}$$

$$= \sum_{p = a \bmod N} \frac{\varphi(N) \, \log p}{p^s} + \sum_{\chi \bmod N} \chi(a) \sum_{p \not| N \text{ prime}, m \geq 2} \frac{\log p}{\chi(p)^m \, p^{ms}}$$

We do not care about whether cancellation does or does not occur in the second sum. All that we care is that it is absolutely convergent for $\mathrm{Re}(s) > \frac{1}{2}$. To see this we do *not* need any subtle information about primes, but, rather, dominate the sum over primes by the corresponding sum over integers ≥ 2. Namely,

$$\left| \sum_{p \not| N \text{ prime}, m \geq 2} \frac{\log p}{\chi(p)^m \, p^{ms}} \right| \leq \sum_{n \geq 2,\, m \geq 2} \frac{\log n}{n^{m\sigma}} = \sum_{n \geq 2} \frac{(\log n)/n^{2\sigma}}{1 - n^{-\sigma}} \leq \frac{1}{1 - 2^{-\sigma}} \sum_{n \geq 2} \frac{\log n}{n^{2\sigma}}$$

where $\sigma = \mathrm{Re}(s)$. This converges for $\mathrm{Re}(s) > \frac{1}{2}$.

That is, for $s \longrightarrow 1^+$,

$$- \sum_{\chi \bmod N} \chi(a) \frac{L'(s,\chi)}{L(s,\chi)} \; = \; \varphi(N) \sum_{p = a \bmod N} \frac{\log p}{p^s} \; + \; (\text{something continuous at } s = 1)$$

We have isolated primes $p = a \bmod N$. Thus, as Dirichlet saw, to prove the infinitude of primes $p = a \bmod N$ it would suffice to show that the left-hand side of the last inequality blows up at $s = 1$. In particular, for the **trivial** character $\chi_o \bmod N$, with values

$$\chi(b) = \begin{cases} 1 & (\text{for } \gcd(b, N) = 1) \\ 0 & (\text{for } \gcd(b, N) > 1) \end{cases}$$

the associated L-function is barely different from the zeta function, namely

$$L(s, \chi_o) = \zeta(s) \cdot \prod_{p|N} \left(1 - \frac{1}{p^s}\right)$$

Since none of those finitely-many factors for primes dividing N is 0 at $s = 1$, $L(s, \chi_o)$ still blows up at $s = 1$.

By contrast, we will show below that for **non-trivial** character $\chi \bmod N$, $\lim_{s \longrightarrow 1^+} L(s, \chi)$ is *finite*, and

$$\lim_{s \longrightarrow 1^+} L(s, \chi) \neq 0$$

Thus, for non-trivial character, the logarithmic derivative is finite and non-zero at $s = 1$. Putting this all together, we will have

$$\lim_{s \longrightarrow 1^+} - \sum_{\chi \bmod N} \chi(a) \frac{L'(s,\chi)}{L(s,\chi)} = +\infty$$

Then necessarily

$$\lim_{s \longrightarrow 1^+} \varphi(N) \sum_{p = a \bmod N} \frac{\log p}{p^s} = +\infty$$

and there must be infinitely many primes $p = a \bmod N$. ///

[2.0.4] **Remark:** The non-vanishing of the non-trivial L-functions at 1, which we prove a bit further belo, is a crucial technical point.

3. *Dual groups of abelian groups*

Before worrying about the non-vanishing of L-functions at $s = 1$ for non-trivial characters χ, we explain Dirichlet's innovation, the use of group characters to isolate primes in a specified congruence class modulo N.

These ideas were the predecessors of the group theory work of Frobenious and Schur 50 years later, and one of the ancestors of *representation theory* of groups.

The **dual group** or **group of characters** $\widehat{G}$ of a finite abelian group G is by definition

$$\widehat{G} = \{\text{group homomorphisms } \chi : G \longrightarrow \mathbb{C}^\times\}$$

This $\widehat{G}$ is itself an abelian group under the operation on characters defined for $g \in G$ by

$$(\chi_1 \cdot \chi_2)(g) = \chi_1(g) \cdot \chi_2(g)$$

[3.0.1] **Proposition:** Let G be a cyclic group of order n with specified generator g_1. Then $\widehat{G}$ is isomorphic to the group of complex n^{th} roots of unity, by

$$(g_1 \longrightarrow \zeta) \longleftarrow \zeta$$

That is, an n^{th} root of unity ζ gives the character χ such that

$$\chi(g_1^\ell) = \zeta^\ell$$

In particular, $\widehat{G}$ is cyclic of order n.

Proof: First, the value of a character χ on g_1 determines all values of χ, since g_1 is a generator for G. And since $g_1^n = e$,

$$\chi(g_1)^n = \chi(g_1^n) = \chi(e) = 1$$

it follows that the only possible values of $\chi(g_1)$ are n^{th} roots of unity. At the same time, for an n^{th} root of unity ζ the formula

$$\chi(g_1^\ell) = \zeta^\ell$$

does give a *well-defined* function on G, since the ambiguity on the right-hand side is by changing ℓ by multiples of n, but g_1^ℓ does only depend upon $\ell \bmod n$. Since the formula gives a well-defined function, it gives a homomorphism, hence, a character. ///

[3.0.2] **Proposition:** Let $G = A \oplus B$ be a direct sum of finite abelian groups. Then there is a *natural* isomorphism of the dual groups

$$\widehat{G} \approx \widehat{A} \oplus \widehat{B}$$

by

$$((a \oplus b) \longrightarrow \chi_1(a) \cdot \chi_2(b)) \quad \longleftarrow \quad \chi_1 \oplus \chi_2$$

Proof: The indicated map is certainly an injective homomorphism of abelian groups. To prove surjectivity, let χ be an arbitrary element of $\widehat{G}$. Then for $a \in A$ and $b \in B$

$$\chi_1(a) = \chi(a \oplus 0) \qquad \chi_2(a) = \chi(0 \oplus b)$$

gives a pair of characters χ_1 and χ_2 in $\widehat{A}$ and $\widehat{B}$. Unsurprisingly, $\chi_1 \oplus \chi_2$ maps to the given χ, proving surjectivity. ///

[3.0.3] Corollary: Invoking the Structure Theorem for finite abelian groups, write a finite abelian group G as

$$G \approx \mathbb{Z}/d_1 \oplus \ldots \mathbb{Z}/d_t$$

for some elementary divisors d_i. [6] Then

$$\widehat{G} \approx \widehat{\mathbb{Z}/d_1} \oplus \ldots \widehat{\mathbb{Z}/d_t} \approx \mathbb{Z}/d_1 \oplus \ldots \mathbb{Z}/d_t \approx G$$

In particular,

$$|\widehat{G}| = |G|$$

Proof: The leftmost of the three isomorphisms is the assertion of the previous proposition. The middle isomorphism is the sum of isomorphisms of the form (for $d \neq 0$ and integer)

$$\widehat{\mathbb{Z}/d} \approx \mathbb{Z}/d$$

proven just above in the guise of cyclic groups. ///

[3.0.4] Proposition: Let G be a finite abelian group. For $g \neq e$ in G, there is a character $\chi \in \widehat{G}$ such that $\chi(g) \neq 1$. [7]

Proof: Again expressing G as a sum of cyclic groups

$$G \approx \mathbb{Z}/d_1 \oplus \ldots \mathbb{Z}/d_t$$

given $g \neq e$ in G, there is some index i such that the projection g_i of g to the i^{th} summand $\mathbb{Z}/d_i$ is non-zero. If we can find a character on $\mathbb{Z}/d_i$ which gives value $\neq 1$ on g_i, then we are done. And, indeed, sending a generator of $\mathbb{Z}/d_i$ to a *primitive* d_i^{th} root of unity sends every non-zero element of $\mathbb{Z}/d_i$ to a complex number other than 1. ///

[3.0.5] Corollary: *(Dual version of cancellation trick)* For g in a finite abelian group,

$$\sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} |G| & (\text{for } g = e) \\ 0 & (\text{otherwise}) \end{cases}$$

Proof: If $g = e$, then the sum counts the characters in $\widehat{G}$. From just above,

$$|\widehat{G}| = |G|$$

On the other hand, given $g \neq e$ in G, by the previous proposition let χ_1 be in $\widehat{G}$ such that $\chi_1(g) \neq 1$. The map on $\widehat{G}$

$$\chi \longrightarrow \chi_1 \cdot \chi$$

is a bijection of $\widehat{G}$ to itself, so

$$\sum_{\chi \in \widehat{G}} \chi(g) = \sum_{\chi \in \widehat{G}} (\chi \cdot \chi_1)(g) = \chi_1(g) \cdot \sum_{\chi \in \widehat{G}} \chi(g)$$

[6] We do not need to know that $d_1 | \ldots | d_t$ for present purposes.

[7] This idea that characters can distinguish group elements from each other is just the tip of an iceberg.

which gives

$$(1-\chi_1(g)) \cdot \sum_{\chi \in \widehat{G}} \chi(g) = 0$$

Since $1-\chi_1(g) \neq 0$, it must be that the sum is 0. ///

4. *Non-vanishing on* $\mathrm{Re}(s) = 1$

Dirichlet's argument for the infinitude of primes $p = a \bmod N$ (for $\gcd(a, N) = 1$) requires that $L(1, \chi) \neq 0$ for all $\chi \bmod N$. We prove this now, granting that these functions have meromorphic extensions to some neighborhood of $s = 1$. We also need to know that for the trivial character $\chi_o \bmod N$ the L-function $L(s, \chi_o)$ has a *simple* pole at $s = 1$. These analytical facts are proven in the next section.

[4.0.1] **Theorem:** For a Dirichlet character $\chi \bmod N$ other than the trivial character $\chi_o \bmod N$,

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

Proof: To prove that the L-functions $L(s, \chi)$ do not vanish at $s = 1$, and in fact do not vanish on the whole line[8] $\mathrm{Re}(s) = 1$, any direct argument involves a trick similar to what we do here. [9]

For χ whose square is not the trivial character χ_o modulo N, the standard trick is to consider

$$\lambda(s) = L(s, \chi_o)^3 \cdot L(s, \chi)^4 \cdot L(s, \chi^2)$$

Then, letting $\sigma = \mathrm{Re}(s)$, from the Euler product expressions for the L-functions noted earlier, in the region of convergence,

$$|\lambda(s)| = |\exp\left(\sum_{m,p} \frac{3 + 4\chi(p^m) + \chi^2(p^m)}{mp^{ms}}\right)| = \exp\left|\sum_{m,p} \frac{3 + 4\cos\theta_{m,p} + \cos 2\theta_{m,p}}{mp^{m\sigma}}\right|$$

where for each m and p we let

$$\theta_{m,p} = (\text{the argument of } \chi(p^m)) \in \mathbb{R}$$

The trick[10] is that for *any* real θ

$$3 + 4\cos\theta + \cos 2\theta = 3 + 4\cos\theta + 2\cos^2\theta - 1 = 2 + 4\cos\theta + 2\cos^2\theta = 2(1+\cos\theta)^2 \geq 0$$

Therefore, all the terms inside the large sum being exponentiated are non-negative, and,[11]

$$|\lambda(s)| \geq e^0 = 1$$

[8] Non-vanishing of $\zeta(s)$ on the whole line $\mathrm{Re}(s) = 1$ yields the Prime Number Theorem: let $\pi(x)$ be the number of primes less than x. Then $\pi(x) \sim x/\ln x$, meaning that the limit of the ratio of the two sides as $x \longrightarrow \infty$ is 1. This was first proven in 1896, separately, by Hadamard and de la Vallée Poussin. The same sort of argument also gives an analogous *asymptotic* statement about primes in each congruence class modulo N, namely that $\pi_{a,N}(x) \sim x/[\varphi(N) \cdot \ln x]$, where $\gcd(a, N) = 1$ and φ is Euler's totient function.

[9] A more natural (and dignified) but considerably more demanding argument for non-vanishing would entail following the Maaß-Selberg discussion of the spectral decomposition of $SL(2, \mathbb{Z}) \backslash SL(2, \mathbb{R})$.

[10] Presumably found after considerable fooling around.

[11] Miraculously...

In particular, if $L(1,\chi) = 0$ were to be 0, then, since $L(s,\chi_o)$ has a simple pole at $s = 1$ and since $L(s,\chi^2)$ does *not* have a pole (since $\chi^2 \neq \chi_o$), the multiplicity ≥ 4 of the 0 in the product of L-functions would overwhelm the three-fold pole, and $\lambda(1) = 0$. This would contradict the inequality just obtained.

For $\chi^2 = \chi_o$, instead consider

$$\lambda(s) = L(s,\chi) \cdot L(s,\chi_o) = \exp\left(\sum_{p,m} \frac{1+\chi(p^m)}{mp^{ms}}\right)$$

If $L(1,\chi) = 0$, then this would cancel the simple pole of $L(s,\chi_o)$ at 1, giving a non-zero finite value at $s = 1$. The series inside the exponentiation is a Dirichlet series with non-negative coefficients, and for real s

$$\sum_{p,m} \frac{1+\chi(p^m)}{mp^{ms}} \geq \sum_{p,\, m \text{ even}} \frac{1+1}{mp^{ms}} = \sum_{p,\, m} \frac{1+1}{2mp^{2ms}} = \sum_{p,\, m} \frac{1}{mp^{2ms}} = \log\zeta(2s)$$

Since $\zeta(2s)$ has a simple pole at $s = \frac{1}{2}$ the series

$$\log\left(L(s,\chi) \cdot L(s,\chi_o)\right) = \sum_{p,m} \frac{1+\chi(p^m)}{mp^{ms}} \geq \log\zeta(2s)$$

necessarily blows up as $s \longrightarrow \frac{1}{2}^+$. But by **Landau's Lemma** (in the next section), a Dirichlet series with non-negative coefficients cannot blow up as $s \longrightarrow s_o$ along the real line unless the function represented by the series fails to be holomorphic at s_o. Since the function given by $\lambda(s)$ is holomorphic at $s = 1/2$, this gives a contradiction to the supposition that $\lambda(s)$ is holomorphic at $s = 1$ (which had allowed this discussion at $s = 1/2$). That is, $L(1,\chi) \neq 0$. ///

5. *Analytic continuations*

Dirichlet's original argument did not emphasize holomorphic functions, but by now we know that discussion of vanishing and blowing-up of functions is most clearly and simply accomplished if the functions are meromorphic when viewed as functions of a complex variable.

For the purposes of Dirichlet's theorem, it suffices to meromorphically continue [12] the L-functions to $\mathrm{Re}(s) > 0$. [13]

[5.0.1] **Theorem:** The Dirichlet L-functions

$$L(s,\chi) = \sum_n \frac{\chi(n)}{n^s} = \prod_p \frac{1}{1-\chi(p)\,p^{-s}}$$

[12] An extension of a holomorphic function to a larger region, on which it may have some poles, is called a **meromorphic continuation**. There is *no* general methodology for proving that functions have meromorphic continuations, due in part to the fact that, generically, functions *do not* have continuations beyond some natural region where they're defined by a convergent series or integral. Indeed, to be able to prove a meromorphic continuation result for a given function is tantamount to proving that it has some deeper significance.

[13] Already prior to Riemann's 1858 paper, it was known that the Euler-Riemann zeta function and all the L-functions we need here did indeed have meromorphic continuations to the whole complex plane, have no poles unless the character χ is trivial, and have functional equations similar to that of zeta, namely that $\pi^{-s/2}\Gamma(s/2)\zeta(s)$ is invariant under $s \longrightarrow 1-s$.

have meromorphic continuations to $\mathrm{Re}(s) > 0$. For χ non-trivial, $L(s, \chi)$ is *holomorphic* on that half-plane. For χ trivial, $L(s, \chi_o)$ has a *simple* pole at $s = 1$ and is holomorphic otherwise.

Proof: First, to treat the trivial character χ_o mod N, recall, as already observed, that the corresponding L-function differs in an elementary way from $\zeta(s)$, namely

$$L(s, \chi_o) = \zeta(s) \cdot \prod_{p|N} \left(1 - \frac{1}{p^s}\right)$$

Thus, we analytically continue $\zeta(s)$ instead of $L(s, \chi_o)$. To analytically continue $\zeta(s)$ to $\mathrm{Re}(s) > 0$ observe that the sum for $\zeta(s)$ is fairly well approximated by a more elementary function

$$\zeta(s) - \frac{1}{s-1} = \sum_{n=1}^{\infty} \frac{1}{n^s} - \int_1^{\infty} \frac{dx}{x^s} = \sum_{n=1}^{\infty} \left[\frac{1}{n^s} - \frac{\left(\frac{1}{n^{s-1}} - \frac{1}{(n+1)^{s-1}}\right)}{1-s} \right]$$

Since

$$\frac{\left(\frac{1}{n^{s-1}} - \frac{1}{(n+1)^{s-1}}\right)}{1-s} = \frac{1}{n^s} + O(\frac{1}{n^{s+1}})$$

with a uniform O-term, we obtain

$$\zeta(s) - \frac{1}{s-1} = \sum_n O(\frac{1}{n^{s+1}}) = \text{holomorphic for } \mathrm{Re}(s) > 0$$

The obvious analytic continuation of $1/(s-1)$ allows analytic continuation of $\zeta(s)$.

A relatively elementary analytic continuation argument for *non-trivial* characters uses **partial summation**. That is, let $\{a_n\}$ and $\{b_n\}$ be sequences of complex numbers such that the partial sums $A_n = \sum_{i=1}^n a_i$ are *bounded*, and $b_n \longrightarrow 0$. Then it is useful to rearrange (taking $A_0 = 0$ for notational convenience)

$$\sum_{n=1}^{\infty} a_n b_n = \sum_{n=1}^{\infty} (A_n - A_{n-1}) b_n = \sum_{n=0}^{\infty} A_n b_n - \sum_{n=0}^{\infty} A_n b_{n+1} = \sum_{n=0}^{\infty} A_n (b_n - b_{n+1})$$

Taking $a_n = \chi(n)$ and $b_n = 1/n^s$ gives

$$L(s, \chi) = \sum_{n=0}^{\infty} \left(\sum_{i=1}^{n} \chi(n) \right) (\frac{1}{n^s} - \frac{1}{(n+1)^s})$$

The difference $1/n^s - 1/(n+1)^s$ is s/n^{s+1} up to higher-order terms, so this expression gives a holomorphic function for $\mathrm{Re}(s) > 0$. ///

6. *Dirichlet series with positive coefficients*

Now we prove Landau's result on Dirichlet series with positive coefficients. (More precisely, the coefficients are *non-negative*.)

[6.0.1] **Theorem:** *(Landau)* Let

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

be a Dirichlet series with real coefficients $a_n \geq 0$. Suppose that the series defining $f(s)$ converges for $\mathrm{Re}(s) > \sigma_o$. Suppose further that the function f extends to a function holomorphic in a neighborhood of $s = \sigma_o$. Then, in fact, the series defining $f(s)$ converges for $\mathrm{Re}(s) > \sigma_o - \varepsilon$ for some $\varepsilon > 0$.

Proof: First, by replacing s by $s - \sigma_o$ we lighten the notation by reducing to the case that $\sigma_o = 0$. Since the function $f(s)$ given by the series is holomorphic on $\mathrm{Re}(s) > 0$ and on a neighborhood of 0, there is $\varepsilon > 0$ such that $f(s)$ is holomorphic on $|s-1| < 1+2\varepsilon$, and the power series for the function converges nicely on this open disk. Differentiating the original series termwise, we evaluate the derivatives of $f(s)$ at $s = 1$ as

$$f^{(i)}(1) = \sum_n \frac{(-\log n)^i \, a_n}{n} = (-1)^i \sum_n \frac{(\log n)^i \, a_n}{n}$$

and Cauchy's formulas yield, for $|s-1| < 1+2\varepsilon$,

$$f(s) = \sum_{i \geq 0} \frac{f^{(i)}(1)}{i!} \, (s-1)^i$$

In particular, for $s = -\varepsilon$, we are assured of the convergence to $f(-\varepsilon)$ of

$$f(-\varepsilon) = \sum_{i \geq 0} \frac{f^{(i)}(1)}{i!} \, (-\varepsilon - 1)^i$$

Note that $(-1)^i f^{(i)}(1)$ is a positive Dirichlet series, so we move the powers of -1 a little to obtain

$$f(-\varepsilon) = \sum_{i \geq 0} \frac{(-1)^i f^{(i)}(1)}{i!} \, (\varepsilon + 1)^i$$

The series

$$(-1)^i f^{(i)}(1) = \sum_n (\log n)^i \, \frac{a_n}{n}$$

has positive terms, so the double series (convergent, with positive terms)

$$f(-\varepsilon) = \sum_{n,i} \frac{a_n \, (\log n)^i}{i!} (1+\varepsilon)^i \frac{1}{n}$$

can be rearranged to

$$f(-\varepsilon) = \sum_n \frac{a_n}{n} \left(\sum_i \frac{(\log n)^i (1+\varepsilon)^i}{i!} \right) = \sum_n \frac{a_n}{n} n^{(1+\varepsilon)} = \sum_n \frac{a_n}{n^{-\varepsilon}}$$

That is, the latter series converges (absolutely). ///