DIRICHLET'S THEOREM ON ARITHMETIC PROGRESSIONS

1. Introduction

Question: *Let a, N be integers with $0 \leq a < N$ and $\gcd(a, N) = 1$. Does the arithmetic progression*

$$\{a, a+N, a+2N, a+3N, \dots\}$$

contain infinitely many primes?

For example, if $a = 4$, $N = 15$, does the arithmetic progression

$$\{4, 19, 34, 49, \dots\}$$

contain infinitely many primes?

Answer (Dirichlet, 1837): *Yes. Further, for fixed N the primes distribute evenly among the arithmetic progressions for all such a.*

For example, if $N = 15$, eight arithmetic progressions are candidates to contain primes:

$$\begin{gathered}
\{1, 1+15, 1+2\cdot 15, 1+3\cdot 15, \dots\}, \\
\{2, 2+15, 2+2\cdot 15, 2+3\cdot 15, \dots\}, \\
\{4, 4+15, 4+2\cdot 15, 4+3\cdot 15, \dots\}, \\
\{7, 7+15, 7+2\cdot 15, 7+3\cdot 15, \dots\}, \\
\{8, 8+15, 8+2\cdot 15, 8+3\cdot 15, \dots\}, \\
\{11, 11+15, 11+2\cdot 15, 11+3\cdot 15, \dots\}, \\
\{13, 13+15, 13+2\cdot 15, 13+3\cdot 15, \dots\}, \\
\{14, 14+15, 14+2\cdot 15, 14+3\cdot 15, \dots\}.
\end{gathered}$$

In fact, each of these progressions contains infinitely many primes, and the primes distribute evenly among them. The phrase *distribute evenly* will be defined more precisely later on.

Contents

1. Introduction 1
2. Euler's proof of infinitely many primes 2
3. Dirichlet characters 3
4. More on Dirichlet characters 5
5. Yet more on Dirichlet characters 6
6. L-functions and the first idea of Dirichlet's proof 7
7. Analytic properties of $L(\chi, s)$ 7
8. The second idea of Dirichlet's proof 8
9. Meromorphy of $\zeta_N(s)$ at $s = 1$ 9
10. Review of the proofs 11
11. Place-holder continuation arguments 12

2. Euler's proof of infinitely many primes

Recall some formulas:

- Geometric series:
$$\sum_{m=0}^{\infty} X^m = (1-X)^{-1}, \quad X \in \mathbb{C},\ |X| < 1,$$
- Logarithm series:
$$\log(1-X)^{-1} = \sum_{m=1}^{\infty} m^{-1} X^m, \quad X \in \mathbb{C},\ |X| < 1,$$
- Telescoping series:
$$\sum_{m=2}^{\infty} \frac{1}{m(m-1)} = 1.$$
(Proof: $\frac{1}{m(m-1)} = \frac{1}{m-1} - \frac{1}{m}$.)

First we establish Euler's identity, in which $\mathcal{P}$ denotes the set of prime numbers,
$$\sum_{n \in \mathbb{Z}^+} n^{-s} = \prod_{p \in \mathcal{P}} (1-p^{-s})^{-1}, \quad s > 1.$$
The Fundamental Theorem of Arithmetic asserts that any $n \in \mathbb{Z}^+$ is uniquely expressible as $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r} \dots$ with all $e_i \in \mathbb{N}$ and almost all $e_i = 0$. Euler's identity really just rephrases this fact:
$$\begin{aligned}
\sum_{n=2^e} n^{-s} &= \sum_{e=0}^{\infty} (2^{-s})^e = (1-2^{-s})^{-1}, \\
\sum_{n=2^{e_1}3^{e_2}} n^{-s} &= \sum_{e_1=0}^{\infty} (2^{-s})^{e_1} \sum_{e_2=0}^{\infty} (3^{-s})^{e_2} = (1-2^{-s})^{-1}(1-3^{-s})^{-1}, \\
&\vdots \\
\sum_{n=2^{e_1}\cdots p_r^{e_r}} n^{-s} &= \prod_{i=1}^{r} \sum_{e_i=0}^{\infty} (p_i^{-s})^{e_i} = \prod_{i=1}^{r} (1-p_i^{-s})^{-1}, \\
&\vdots \\
\sum_{n \in \mathbb{Z}^+} n^{-s} &= \prod_{p \in \mathcal{P}} (1-p^{-s})^{-1}.
\end{aligned}$$
With Euler's identity in place, his proof that there are infinitely many primes follows. Let
$$\zeta(s) = \sum_{n \in \mathbb{Z}^+} n^{-s} = \prod_{p \in \mathcal{P}} (1-p^{-s})^{-1}, \quad s > 1.$$
By the product expansion of ζ,
$$\log \zeta(s) = \log \prod_{p \in \mathcal{P}} (1-p^{-s})^{-1} = \sum_{p \in \mathcal{P}} \log(1-p^{-s})^{-1} = \sum_{p \in \mathcal{P}} \sum_{m=1}^{\infty} m^{-1} p^{-ms}.$$

That is,

$$\log \zeta(s) = \sum_{p \in \mathcal{P}} p^{-s} + \sum_{p \in \mathcal{P}} \sum_{m=2}^{\infty} m^{-1} p^{-ms}.$$

But the second term in the previous display is small by a basic estimate, then the geometric sum formula, then comparison with the telescoping series,

$$\sum_{p \in \mathcal{P}} \sum_{m=2}^{\infty} m^{-1} p^{-ms} < \sum_{p \in \mathcal{P}} \sum_{m=2}^{\infty} p^{-m} = \sum_{p \in \mathcal{P}} \frac{1}{p^2(1-p^{-1})} = \sum_{p \in \mathcal{P}} \frac{1}{p(p-1)} < 1.$$

And so

$$\sum_{p \in \mathcal{P}} p^{-s} = \log \zeta(s) + \varepsilon, \quad |\varepsilon| < 1.$$

By the sum expansion of ζ, $\lim_{s \to 1^+} \zeta(s) = \infty$ because the harmonic series diverges. So $\lim_{s \to 1^+} \log \zeta(s) = \infty$, and thus

$$\lim_{s \to 1^+} \sum_{p \in \mathcal{P}} p^{-s} = \infty.$$

The only way for the sum to diverge is if it is over an infinite set of summands, so there must be infinitely many primes.

3. Dirichlet characters

Dirichlet augmented Euler's idea by using Fourier analysis to pick off only the primes p such that $p \equiv a \pmod N$.

Let

$$G = (\mathbb{Z}/N\mathbb{Z})^\times,$$

a finite abelian multiplicative group of order

$$|G| = \phi(N) \quad \text{where } \phi \text{ is Euler's totient function.}$$

Define

$$G^* = \{\text{homomorphisms} : G \longrightarrow \mathbb{C}^\times\}.$$

Then G^* forms a finite abelian multiplicative group also. Specifically, for any $\chi_1, \chi_2 \in G^*$, define $\chi_1\chi_2$ by the rule

$$(\chi_1\chi_2)(g) = \chi_1(g)\chi_2(g), \quad g \in G.$$

The identity element of G^* is the character χ such that $\chi(g) = 1$ for all $g \in G$, and we use the symbol 1 (or 1_N to emphasize N) to denote this character. The group G^* is called the *dual group* of G. One can show that $G^* \cong G$ by using the elementary divisor structure of finite abelian groups (or by using the Sun Ze theorem and the structure of the groups $(\mathbb{Z}/p^e\mathbb{Z})^\times$), but the isomorphism is not canonical.

Proposition 3.1 (Orthogonality Relations). *For each $\chi \in G^*$,*

$$\sum_{g \in G} \chi(g) = \begin{cases} |G| & \text{if } \chi = 1, \\ 0 & \text{otherwise,} \end{cases}$$

And for each $g \in G$,

$$\sum_{\chi \in G^*} \chi(g) = \begin{cases} |G| & \text{if } g = 1, \\ 0 & \text{otherwise.} \end{cases}$$

For the second orthogonality relation, an argument is needed that if $g \neq 1_G$ then there is a character $\chi \in G^*$ such that $\chi(g) \neq 1_{\mathbb{C}}$. We will address this point later in this writeup.

For any function $f : G \longrightarrow \mathbb{C}$, the *Fourier transform* of f is a corresponding function on the dual group,

$$\widehat{f} : G^* \longrightarrow \mathbb{C}, \qquad \widehat{f}(\chi) = \frac{1}{\phi(N)} \sum_{x \in G} f(x)\chi(x^{-1}),$$

and then the *Fourier series* of f is

$$s_f : G \longrightarrow \mathbb{C}, \qquad s_f = \sum_{\chi \in G^*} \widehat{f}(\chi)\chi.$$

The second orthogonality relation shows that the Fourier series synthesizes the original function,

$$\begin{aligned} s_f(x) &= \sum_{\chi \in G^*} \frac{1}{\phi(N)} \sum_{y \in G} f(y)\chi(y^{-1})\chi(x) \\ &= \sum_{y \in G} f(y) \frac{1}{\phi(N)} \sum_{\chi \in G^*} \chi(xy^{-1}) = f(x). \end{aligned}$$

Because the group G is finite, no qualifications on the function f, and no convergence issues of any sort, are involved here.

Returning to the Dirichlet proof, specialize the function $f : G \longrightarrow \mathbb{C}$ to the indicator function δ_a that picks off $a \pmod N$,

$$\delta_a(x) = \begin{cases} 1 & \text{if } x = a, \\ 0 & \text{otherwise.} \end{cases}$$

Then for any $\chi \in G^*$, the χth Fourier coefficient $1/\phi(N) \sum_{x \in G} \delta_a(x)\chi(x^{-1})$ of δ_a is simply

$$\widehat{\delta}_a(\chi) = \frac{1}{\phi(N)} \chi(a^{-1}),$$

and so the Fourier series synthesis of δ_a,

$$\delta_a = \frac{1}{\phi(N)} \sum_{\chi} \chi(a^{-1})\chi,$$

is inevitably just the second orthogonality relation,

$$\frac{1}{\phi(N)} \sum_{\chi \in G^*} \chi(xa^{-1}) = \begin{cases} 1 & \text{if } x = a, \\ 0 & \text{otherwise.} \end{cases}$$

The Dirichlet proof is concerned with the sum $\sum_{p \equiv a(N)} p^{-s}$. The indicator function δ_a lets us take a sum over all primes instead and then replace δ_a by its Fourier series from the penultimate display, obtaining

$$\sum_{p \equiv a(N)} p^{-s} = \sum_{p \in \mathcal{P}} \delta_a(p)p^{-s} = \frac{1}{\phi(N)} \sum_{\chi \in G^*} \chi(a^{-1}) \sum_{p \in \mathcal{P}} \chi(p)p^{-s}.$$

We will return to this formula soon.

4. More on Dirichlet characters

Associate to any character $\chi \in G^*$ a corresponding function from $\mathbb{Z}$ to $\mathbb{C}$, also called χ, as follows. First, there exists a least positive divisor M of N such that χ factors as

$$\chi = \chi_o \circ \pi_M : (\mathbb{Z}/N\mathbb{Z})^\times \xrightarrow{\pi_M} (\mathbb{Z}/M\mathbb{Z})^\times \xrightarrow{\chi_o} \mathbb{C}^\times.$$

The integer M is the *conductor* of χ, and the character χ_o is *primitive*. Note that

$$\chi_o(n + M\mathbb{Z}) = \chi(n + N\mathbb{Z}) \quad \text{if } \gcd(n, N) = 1,$$

but if $\gcd(n, M) = 1$ while $\gcd(n, N) > 1$ then $\chi_o(n + M\mathbb{Z})$ is defined and nonzero even though $\chi(n + N\mathbb{Z})$ is undefined. Second, redefine the original symbol χ to denote the primitive character χ_o lifted to a multiplicative function on the positive integers,

$$\chi : \mathbb{Z}^+ \longrightarrow \mathbb{C}, \quad \chi(n) = \begin{cases} \chi_o(n + M\mathbb{Z}) & \text{if } \gcd(n, M) = 1, \\ 0 & \text{if } \gcd(n, M) > 1. \end{cases}$$

The following relation, with the new χ on the left and the original χ on the right,

$$\chi(n) = \chi(n + N\mathbb{Z}) \quad \text{if } \gcd(n, N) = 1,$$

justifies the multiple use of the symbol χ. For example, the orthogonality relations are undisturbed if we apply the new χ to coset representatives rather than applying the original χ to cosets. For $\gcd(n, N) > 1$, $\chi(n)$ is defined and possibly nonzero, while $\chi(n + N\mathbb{Z})$ is undefined. By default, we pass all Dirichlet characters through the process described here, suppressing further reference to χ_o from the notation.

In particular, if $N > 1$ then the trivial character $1_N \in G^*$ does not lift directly to the constant function 1 on the positive integers. However, 1_N has conductor $M = 1$, and the primitive trivial character 1 modulo 1 is identically 1 on $(\mathbb{Z}/1\mathbb{Z})^\times = \{\overline{0}\}$. The primitive trivial character lifts to the constant function $1(n) = 1$ for all $n \in \mathbb{Z}^+$.

For another example, the Dirichlet character $\chi : (\mathbb{Z}/12\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$ given by

$$1 + 12\mathbb{Z} \mapsto 1, \quad 5 + 12\mathbb{Z} \mapsto -1, \quad 7 + 12\mathbb{Z} \mapsto 1, \quad 11 + 12\mathbb{Z} \mapsto -1$$

factors through the map $\pi_3 : (\mathbb{Z}/12\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/3\mathbb{Z})^\times$, which takes $1 + 12\mathbb{Z}$ and $7 + 12\mathbb{Z}$ to $1 + 3\mathbb{Z}$ and takes $5 + 12\mathbb{Z}$ and $11 + 12\mathbb{Z}$ to $2 + 3\mathbb{Z}$, with the resulting primitive character $\chi_o : (\mathbb{Z}/3\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$ being

$$1 + 3\mathbb{Z} \mapsto 1, \quad 2 + 3\mathbb{Z} \mapsto -1.$$

Now the redefined $\chi : \mathbb{Z}^+ \longrightarrow \mathbb{C}$ is

$$\chi(n) = \begin{cases} 0 & \text{if } n \equiv 0 \pmod 3, \\ 1 & \text{if } n \equiv 1 \pmod 3, \\ -1 & \text{if } n \equiv 2 \pmod 3. \end{cases}$$

Overall there are four Dirichlet characters modulo 12, having conductors 1, 3, 4, and 12, as follows. For each character $\chi = \chi_m$, having conductor m, the first four columns are values $\chi(a + 12\mathbb{Z})$ while the fifth column gives the nonzero values of χ

after it is made primitive and then lifted to $\mathbb{Z}^+$.

	1	5	7	11	nonzero values of χ on $\mathbb{Z}^+$
χ_1	1	1	1	1	$\mathbb{Z}^+ \mapsto 1$
χ_3	1	-1	1	-1	$1+3\mathbb{Z}_{\geq 0} \mapsto 1,\ 2+3\mathbb{Z}_{\geq 0} \mapsto -1$
χ_4	1	1	-1	-1	$1+4\mathbb{Z}_{\geq 0} \mapsto 1,\ 3+4\mathbb{Z}_{\geq 0} \mapsto -1$
χ_{12}	1	-1	-1	1	$\{1,11\}+12\mathbb{Z}_{\geq 0} \mapsto 1,\ \{5,7\}+12\mathbb{Z}_{\geq 0} \mapsto -1$

The orthogonality relations say that the four rows of character values at 1, 5, 7, and 11 form an (essentially) orthogonal matrix, and because the first row entries are all 1 the entries of each other row sum to 0. We will return to the Dirichlet characters modulo 12 later in this writeup.

5. Yet more on Dirichlet characters

Proposition 5.1. *Let G be a finite abelian group, written additively, and let H be a subgroup. Suppose that $\chi : H \longrightarrow \mathbb{C}^\times$ is a character. Then χ extends to a character of G, and there are $[G:H]$ such extensions.*

Proof. Consider any element g of G that does not lie in H. Some positive integer multiple dg does lie in H, and we take the smallest such d. Consider the direct sum $H \oplus \langle g \rangle$, which need not be a subgroup of G. Consider also the subgroup $\langle -dg \oplus dg \rangle$ of the direct sum. The quotient $(H \oplus \langle g \rangle)/\langle -dg \oplus dg \rangle$ is isomorphic to the subgroup $H + \langle g \rangle$ (nondirect sum) of G, which properly contains H.

Extend χ from H to the direct sum $H \oplus \langle g \rangle$ by defining $\chi(h \oplus 0) = \chi(h)$ for all $h \in H$ and defining $\chi(0 \oplus g)$ to be any complex number whose dth power is $\chi(dg)$; there are d such extensions of χ. This extended χ is trivial on $\langle -dg \oplus dg \rangle$ because $\chi(-dg \oplus dg) = \chi(-dg \oplus 0)\chi(0 \oplus dg) = \chi(dg)^{-1}\chi(0 \oplus g)^d = 1$, and so it descends to the quotient $(H \oplus \langle g \rangle)/\langle -dg \oplus dg \rangle$. That is, the extended χ is defined on the subgroup $H + \langle g \rangle$ of G that properly contains H. The number d of such possible characters is also the index $[H + \langle g \rangle : H]$ of H in $H + \langle g \rangle$.

Repeat the process to extend the character χ until it is defined on all of G. The nature of the construction shows that there are $[G:H]$ extensions. $\square$

As a small example let $G = \mathbb{Z}/4\mathbb{Z}$, notated $\{0,1,2,3\}$, and let $H = \{0,2\}$. Consider the character $\chi : H \longrightarrow \mathbb{C}^\times$ given by $\chi(0) = 1$ and $\chi(2) = -1$. Let $g = 1$, an element of G and not of H but with $2g = 2$ in H. To extend χ to g we must take $\chi(g)$ to be a complex number that squares to $\chi(2)$, either of $\chi(g) = \pm i$. Now χ is a homomorphism from $H \oplus \langle g \rangle = \{0,2\} \oplus \{0,1,2,3\}$ to $\mathbb{C}$, and $\chi(-2 \oplus 2) = \chi((-2 \oplus 0) + (0 \oplus 2)) = \chi(-2 \oplus 0)\chi(0 \oplus 2) = \chi(2)^{-1}\chi(1)^2 = (-1)^{-1}(\pm i)^2 = 1$, so χ is defined on the quotient $(\{0,2\} \oplus \{0,1,2,3\})/\langle -2 \oplus 2 \rangle$, in which $2 \oplus n \equiv 0 \oplus (n+2)$ for $n = 0,1,2,3$, making the quotient isomorphic to G. Thus the extended character is either of $\chi(0) = 1$, $\chi(1) = \pm i$, $\chi(2) = -1$, $\chi(3) = \mp i$.

Now return to the setting of this writeup, with the finite multiplicative abelian group $G = (\mathbb{Z}/N\mathbb{Z})^\times$ for some N. This discussion has shown that any Dirichlet character of any subgroup H of G extends to a Dirichlet character of G, and there are $|G|/|H|$ such extensions. Especially, for any $g \neq 1_G$ in G, the cyclic subgroup H of G generated by g has a character that doesn't take g to 1, and this character extends to a character of G. This observation justifies the observation made earlier in connection with the second orthogonality relation that if $g \neq 1_G$ then there is a character $\chi \in G^*$ such that $\chi(g) \neq 1_{\mathbb{C}}$.

6. L-functions and the first idea of Dirichlet's proof

Recall that $G = (\mathbb{Z}/N\mathbb{Z})^\times$, $a \in G$, and the goal is to show that the set

$$\{p \in \mathcal{P} : p \equiv a \pmod N\}$$

is infinite.

For each $\chi \in G^*$, with its corresponding $\chi : \mathbb{Z}^+ \longrightarrow \mathbb{C}$, define

$$L(\chi, s) = \sum_{n \in \mathbb{Z}^+} \chi(n) n^{-s} = \prod_{p \in \mathcal{P}} (1 - \chi(p) p^{-s})^{-1}, \quad s > 1.$$

The equality of the sum and product follow from a straightforward analogue of the proof of Euler's identity, because characters are homomorphisms. Then

$$\log L(\chi, s) = \sum_{\substack{p \in \mathcal{P} \\ m \in \mathbb{Z}^+}} m^{-1} \chi(p^m) p^{-ms} = \sum_{p \in \mathcal{P}} \chi(p) p^{-s} + \sum_{\substack{p \in \mathcal{P} \\ m \geq 2}} m^{-1} \chi(p^m) p^{-ms},$$

and the second term has absolute value at most 1 by the argument in Euler's proof. Equivalently,

$$\sum_{p \in \mathcal{P}} \chi(p) p^{-s} = \log L(\chi, s) + \varepsilon(\chi), \quad |\varepsilon(\chi)| < 1.$$

Recall the formula that came from the Fourier series of the indicator function of $a \pmod N$,

$$\sum_{p \equiv a(N)} p^{-s} = \frac{1}{\phi(N)} \sum_{\chi} \chi(a^{-1}) \sum_{p \in \mathcal{P}} \chi(p) p^{-s}.$$

The last sum $\sum_p \chi(p) p^{-s}$ in the previous display is the left side of the penultimate display. Thus the previous two displays combine to show that the desired sum is close to the linear combination of $\{\log L(\chi, s)\}$ whose coefficients are the Fourier coefficients of the indicator function,

$$\sum_{p \equiv a(N)} p^{-s} = \frac{1}{\phi(N)} \sum_{\chi} \chi(a^{-1}) \log L(\chi, s) + \varepsilon, \quad |\varepsilon| < 1.$$

This is the first idea of Dirichlet's proof. Now the goal is to show that the right side goes to $+\infty$ as $s \to 1^+$. Already we know that the summand for the trivial character does so. The crux of the matter will be that the finite value $L(\chi, 1)$ for nontrivial χ is *nonzero*. Thus the summands for nontrivial characters are finite, making the sum altogether infinite.

7. Analytic properties of $L(\chi, s)$

We need to study the behavior of $L(\chi, s)$ as $s \to 1^+$. Even though s is real, $L(\chi, s)$ still takes complex values. Bring complex analysis to bear on the matter by viewing s as a complex variable. Begin by extending the definition of $L(\chi)$ to

$$L(\chi, s) = \sum_{n \in \mathbb{Z}^+} \chi(n) n^{-s} = \prod_{p \in \mathcal{P}} (1 - \chi(p) p^{-s})^{-1}, \quad s \in \mathbb{C},\ \mathrm{Re}(s) > 1.$$

Here $n^{-s} = e^{-s \ln n}$ for $n \in \mathbb{Z}^+$. Thus, with $s = \sigma + it$, the size of n^{-s} is $|n^{-s}| = |e^{-(\sigma + it) \ln n}| = |n^{-\sigma} e^{it \ln n}| = n^{-\sigma}$. Consequently the sum expression for $L(\chi, s)$ converges absolutely on the half plane $\{s : \mathrm{Re}(s) > 1\}$, and the convergence is uniform on compacta. Its summands, hence its partial sums, are analytic. So $L(\chi, s)$ is analytic on the half plane.

Proposition 7.1. *The function $L(\chi, s)$ has a meromorphic continuation to the right half plane $\{\mathrm{Re}(s) > 0\}$. If $\chi = 1$ then the extended function $\zeta(s)$ has a simple pole at $s = 1$ with residue 1 and otherwise is analytic. If $\chi \neq 1$ then the extended function $L(\chi, s)$ is analytic.*

Elementary arguments to be given at the end of this writeup establish the proposition. In a separate writeup, results that subsume the proposition are proved by methods that have greater scope.

We reiterate here that the identity

$$\log \zeta(s) \sim \sum_{p \in \mathcal{P}} p^{-s},$$

meaning that

$$\lim_{s \to 1^+} \frac{\log \zeta(s)}{\sum_{p \in \mathcal{P}} p^{-s}} = 1,$$

is the substance of Euler's proof.

8. The second idea of Dirichlet's proof

Recall that for $s > 1$,

$$\sum_{p \equiv a(N)} p^{-s} = \frac{1}{\phi(N)} \sum_{\chi} \chi(a^{-1}) \log L(\chi, s) + \varepsilon, \quad |\varepsilon| < 1.$$

Also, $L(1, s) \to \infty$ as $s \to 1^+$. We will show that for $\chi \neq 1$, $L(\chi, 1) \neq 0$ and thus $\log L(\chi, 1)$ is finite. Because $|\chi(a)^{-1}| = 1$ for all $\chi \in G^*$, it follows that

$$\lim_{s \to 1^+} \left| \sum_{\chi \in G^*} \chi(a)^{-1} \log L(\chi, s) \right| = +\infty$$

and Dirichlet's proof is complete.

We study the function

$$\zeta_N(s) = \prod_{\chi \in G^*} L(\chi, s).$$

Because $L(1, s)$ is meromorphic on $\{s : \mathrm{Re}(s) > 0\}$ with a simple pole at $s = 1$ and all other $L(\chi, s)$ are analytic on $\{s : \mathrm{Re}(s) > 0\}$, there are two possibilities. Either

$$\zeta_N(s) \text{ is meromorphic on } \{s : \mathrm{Re}(s) > 0\} \text{ with a simple pole at } s = 1$$

or

$$\zeta_N(s) \text{ is analytic on } \{s : \mathrm{Re}(s) > 0\}.$$

We will rule out the second possibility to complete the proof.

The function $\zeta_N(s)$ has another definition as the *cyclotomic Dedekind zeta function*. A separate writeup describes $\zeta_N(s)$ this way, but in doing so it must invoke some language and some results from algebraic number theory.

9. Meromorphy of $\zeta_N(s)$ at $s = 1$

Lemma 9.1. *Let p be prime. Let $N = p^d N_p$ with $p \nmid N_p$. Let f_p be the order of p in $(\mathbb{Z}/N_p\mathbb{Z})^\times$,* i.e., *the smallest positive integer such that $p^{f_p} \equiv 1 \pmod{N_p}$. Let $g_p = \phi(N_p)/f_p$. Then for any indeterminate T,*

$$\prod_{\chi \in G^*} (1 - \chi(p)T) = (1 - T^{f_p})^{g_p}.$$

(*See the comment immediately below for a careful parsing of the product in the previous display.*)

On the left side of the equality asserted by the lemma, the expression $\chi(p)$ connotes that the character $\chi \in G^*$ has been reduced to the primitive character χ_o modulo M where $M \mid N$ is the conductor of χ, then lifted M-periodically to $\chi : \mathbb{Z}^+ \longrightarrow \mathbb{C}$, and this is the character that is evaluated at p.

When $p \nmid N$, the process described in the previous paragraph merely reproduces $\chi(p + N\mathbb{Z})$, now referring to the original χ. More generally, the process produces a nonzero value $\chi(p)$ if and only if p does not divide the conductor M of the original χ. That is, the multiplicand $1 - \chi(p)T$ on the left side of the lemma's equality is nontrivial if and only if the original χ factors through $(\mathbb{Z}/N_p\mathbb{Z})^\times$. To repeat: only the characters in G^* that factor through $(\mathbb{Z}/N_p\mathbb{Z})^\times$ contribute something other than 1 to the left side of the lemma's equality. Furthermore, any character in G^* that does factor, $\chi = \chi_{N_p} \circ \pi_{N,N_p}$, is determined by χ_{N_p}. Thus, *to prove the lemma we may consider only characters modulo N_p.*

The subgroup $\langle p + N_p\mathbb{Z}\rangle$ of $(\mathbb{Z}/N_p\mathbb{Z})^\times$ generated by p modulo $N_p\mathbb{Z}$ has f_p characters; specifically, with ρ a primitive f_pth root of unity in $\mathbb{C}$, these characters take $p + N_p\mathbb{Z}$ to ρ^j for $j = 1, \ldots, f_p - 1$. Thus for each j there exist $g_p = \phi(N_p)/f_p$ characters χ modulo N_p that take p to ρ^j. Now the proof of the lemma is immediate.

Proof. Let ρ be a primitive f_pth root of unity in $\mathbb{C}$. Then

$$\prod_{j=0}^{f_p-1} (1 - \rho^j T) = 1 - T^{f_p},$$

and consequently, because g_p characters $\chi \in G^*$ take p to ρ^j for each j,

$$\prod_{\chi \in G^*} (1 - \chi(p)T) = \prod_{j=0}^{f_p-1} (1 - \rho^j T)^{g_p} = (1 - T^{f_p})^{g_p}.$$

$\square$

For example, we confirm the lemma directly for $N = 12$. Recall the four Dirichlet characters modulo 12, having conductors 1, 3, 4, and 12.

	1	5	7	11	nonzero values of χ on $\mathbb{Z}^+$
χ_1	1	1	1	1	$\mathbb{Z}^+ \mapsto 1$
χ_3	1	-1	1	-1	$1 + 3\mathbb{Z}_{\geq 0} \mapsto 1,\ 2 + 3\mathbb{Z}_{\geq 0} \mapsto -1$
χ_4	1	1	-1	-1	$1 + 4\mathbb{Z}_{\geq 0} \mapsto 1,\ 3 + 4\mathbb{Z}_{\geq 0} \mapsto -1$
χ_{12}	1	-1	-1	1	$\{1, 11\} + 12\mathbb{Z}_{\geq 0} \mapsto 1,\ \{5, 7\} + 12\mathbb{Z}_{\geq 0} \mapsto -1$

First consider the prime $p = 2$. We have $1 - \chi_4(2)T = 1$ and $1 - \chi_{12}(2)T = 1$ because 2 divides the conductors; also $1 - \chi_1(2)T = 1 - T$ and $1 - \chi_3(2)T = 1 + T$; so altogether $\prod_{\chi \in G^*}(1 - \chi(2)T) = 1 - T^2$. On the other hand, the values of N_2

and f_2 and g_2 for $N = 12$ are 3 and 2 and 1, and so also $(1 - T^{f_2})^{g_2} = 1 - T^2$, confirming the lemma when $N = 12$ for $p = 2$. Similar arguments work for $p = 3$ with $(N_p, f_p, g_p) = (4, 2, 1)$, for $p \equiv 1 \pmod{12}$ with $(N_p, f_p, g_p) = (12, 1, 4)$, and (together) for $p \equiv 5, 7, 11 \pmod{12}$ with $(N_p, f_p, g_p) = (12, 2, 2)$; because the 5, 7, and 11 columns in the previous table contain the same entries though in different orders, they produce the same value of $\prod_\chi (1 - \chi(p)T)$. The reader can similarly confirm the lemma for $N = 18$; here one character has conductor 1, one has conductor 3, four have conductor 9, and the cases to check are $p = 2$, $p = 3$, $p \equiv 1 \pmod 9$, $p \equiv 2, 5 \pmod 9$, $p \equiv 4, 7 \pmod 9$, $p \equiv 8 \pmod 9$.

In the lemma we could have let $H = (\mathbb{Z}/N_p\mathbb{Z})^\times$, which equals G for all $p \nmid N$, and then stated the lemma's formula as a product over $\chi \in H^*$ rather than worrying about it holding for G^*. Our insistence on G^* pays off in the simplicity of the next proof.

Proposition 9.2. $\zeta_N(s) = \prod_{p \in \mathcal{P}} (1 - p^{-f_p s})^{-g_p}$ *for* $\mathrm{Re}(s) > 1$.

Proof. Compute, using the lemma with $T = p^{-s}$ at the last step,

$$\begin{aligned}\zeta_N(s) = \prod_{\chi \in G^*} L(\chi, s) &= \prod_{\chi \in G^*} \prod_{p \in \mathcal{P}} (1 - \chi(p)p^{-s})^{-1} \\ &= \prod_{p \in \mathcal{P}} \prod_{\chi \in G^*} (1 - \chi(p)p^{-s})^{-1} = \prod_{p \in \mathcal{P}} (1 - p^{-f_p s})^{-g_p}.\end{aligned}$$

The product converges absolutely for $\mathrm{Re}(s) > 1$, justifying the rearrangements. □

For a small example, let $N = 3$. There are two characters modulo 3, the trivial character and the quadratic character $(\cdot/3)$, and so, not yet referring to the proposition,

$$\zeta_3(s) = \prod_{p \in \mathcal{P}} (1 - p^{-s})^{-1}(1 - (p/3)p^{-s})^{-1}.$$

The pth factor is as follows.

- If $p \equiv 1 \pmod 3$ then $(p/3) = 1$ and the pth factor of $\zeta_3(s)$ is $(1 - p^{-s})^{-2}$; this is $(1 - p^{-f_p s})^{-g_p}$ with $f_p = 1$ and $g_p = 2$.
- If $p \equiv 2 \pmod 3$ then $(p/3) = -1$ and the pth factor of $\zeta_3(s)$ is $(1 - p^{-s})^{-1}(1 + p^{-s})^{-1} = (1 - p^{-2s})^{-1}$; this is $(1 - p^{-f_p s})^{-g_p}$ with $f_p = 2$ and $g_p = 1$.
- If $p = 3$ then $(p/3) = 0$ and the pth factor of $\zeta_3(s)$ is $(1 - p^{-s})^{-1}$; this is $(1 - p^{-f_p s})^{-g_p}$ with $f_3 = 1$ and $g_3 = 1$.

We recognize these f and g values from our discussion of factorization in the cubic integer ring $D = \mathbb{Z}[\omega]$, to wit, $p = \prod_{i=1}^g \pi_i^e$ where each π_i has norm $\mathrm{N}\pi = p^f$ and $efg = 2$. Here $e_p = 1$ in the first two cases above, while the value $e_3 = 2$ in the third case plays no role in the pth factor of $\zeta_3(s)$. Recall that in D the primary prime $\lambda = 1 - \omega$ divides 3 with $(e, f, g) = (2, 1, 1)$ (3 is *ramified*), and two nonassociate primary primes divide each $p \equiv 1 \pmod 3$ with $(e, f, g) = (1, 1, 2)$ (p *splits*), and one primary prime divides each $p \equiv 2 \pmod 3$ with $(e, f, g) = (1, 2, 1)$ (p is *inert*).

So we have shown that in fact (with π denoting primary primes in the next display)

$$\begin{aligned}\zeta_3(s) &= \prod_p (1-p^{-f_p s})^{-g_p} \\ &= (1-3^{-s})^{-1} \prod_{p\equiv_3 1} (1-p^{-s})^{-2} \prod_{p\equiv_3 2} (1-p^{-2s})^{-1} \\ &= (1-(\mathrm{N}\lambda)^{-s})^{-1} \prod_{p\equiv_3 1} \prod_{\pi\mid p} (1-(\mathrm{N}\pi)^{-s})^{-1} \prod_{p\equiv_3 2} \prod_{\pi\mid p} (1-(\mathrm{N}\pi)^{-s})^{-1} \\ &= \prod_\pi (1-(\mathrm{N}\pi)^{-s})^{-1}.\end{aligned}$$

That is, $\zeta_3(s) = \prod_\pi (1-(\mathrm{N}\pi)^{-s})^{-1}$ generalizes the original zeta function $\zeta(s) = \prod_p (1-p^{-s})^{-1}$ from $\mathbb{Z}$ to D. Naturally we speculate that $\zeta_N(s)$ similarly extends the original zeta function to $\mathbb{Z}[\zeta_N]$ where $\zeta_N = e^{2\pi i/N}$.

Theorem 9.3. *$\zeta_N(s)$ has a simple pole at $s = 1$. Therefore $L(\chi, 1) \neq 0$ for each nontrivial character χ modulo N.*

Proof. Otherwise $\zeta_N(s)$ is analytic on $\{s : \mathrm{Re}(s) > 0\}$ so that its product expression converges there. But for $s \in \mathbb{R}^+$,

$$(1-p^{-f_p s})^{-g_p} = \left(\sum_{m=0}^{\infty} p^{-mf_p s}\right)^{g_p} \geq \sum_{m=0}^{\infty} p^{-m\phi(N)s} = (1-p^{-\phi(N)s})^{-1}$$

(or one can show the inequality in a more elementary way[1]), and so for $s > 1/\phi(N)$,

$$\zeta_N(s) \geq \prod_{p\in\mathcal{P}} (1-p^{-\phi(N)s})^{-1} = \zeta(\phi(N)s).$$

Now letting s approach $1/\phi(N)$ from the right shows that the product expression of ζ_N diverges there. This gives a contradiction. □

We note that the complex analysis is being treated somewhat loosely here.

10. Review of the proofs

Let the notation $f(s) \sim g(s)$ mean $\lim_{s\to 1^+} f(s)/g(s) = 1$. The three ideas in Euler's proof were

$$\begin{aligned}&\zeta(s) = \sum_{n\in\mathbb{Z}^+} n^{-s} = \prod_{p\in\mathcal{P}} (1-p^{-s})^{-1}, \\ &\sum_{p\in\mathcal{P}} p^{-s} \sim \log\zeta(s), \\ &\lim_{s\to 1^+} \zeta(s) = \infty.\end{aligned}$$

[1] $0 < p^{-f_p s} < 1$, so $0 < p^{-f_p g_p s} \leq p^{-f_p s} < 1$, so $1 > 1 - p^{-f_p g_p s} > 1 - p^{-f_p s} > 0$, so $1 < (1-p^{-f_p g_p s})^{-1} < (1-p^{-f_p s})^{-1} < (1-p^{-f_p s})^{-g_p}$.

The corresponding ideas in Dirichlet's proof were

$$L(\chi, s) = \sum_{n \in \mathbb{Z}^+} \chi(n) n^{-s} = \prod_{p \in \mathcal{P}} (1 - \chi(p) p^{-s})^{-1},$$

$$\sum_{\substack{p \in \mathcal{P} \\ p \equiv a(N)}} p^{-s} \sim \frac{1}{\phi(N)} \sum_{\chi \in G^*} \chi(a)^{-1} \log L(\chi, s),$$

$$\lim_{s \to 1} \zeta_N(s) = \infty \quad \text{where } \zeta_N(s) = \prod_{\chi \in G^*} L(\chi, s).$$

Consequently,

$$\sum_{\substack{p \in \mathcal{P} \\ p \equiv a(N)}} p^{-s} \sim \frac{1}{\phi(N)} \log \zeta(s) \sim \frac{1}{\phi(N)} \sum_{p \in \mathcal{P}} p^{-s}.$$

In other words,

$$\lim_{s \to 1^+} \frac{\sum_{p \equiv a(N)} p^{-s}}{\sum_{p \in \mathcal{P}} p^{-s}} = \frac{1}{\phi(N)}.$$

That is, not only is the set $\{p \in \mathcal{P} : p \equiv a \pmod N\}$ infinite, but furthermore in some limiting sense it contains $1/\phi(N)$ of all the primes. This is the sense in which the primes distribute evenly among the candidate arithmetic progressions $a + N\mathbb{Z}$.

11. Place-holder continuation arguments

One way to continue the Euler–Riemann zeta function from $\{\mathrm{Re}(s) > 1\}$ to $\{\mathrm{Re}(s) > 0\}$ is as follows. Compute that for $\mathrm{Re}(s) > 1$,

$$\zeta(s) - \frac{1}{s-1} = \sum_{n=1}^{\infty} n^{-s} - \int_1^{\infty} t^{-s}\,\mathrm{d}t = \sum_{n=1}^{\infty} \int_n^{n+1} (n^{-s} - t^{-s})\,\mathrm{d}t.$$

This last sum is an infinite sum of analytic functions; call it $\psi(s)$. For positive real s it is the sum of small areas above the $y = t^{-s}$ curve but inside the circumscribing box of the curve over each unit interval, and hence it is bounded absolutely by 1. More generally, for complex s with positive real part we can quantify the smallness of the sum as follows. For all $t \in [n, n+1]$ we have

$$|n^{-s} - t^{-s}| = |s \int_n^t x^{-s-1}\,\mathrm{d}x| \leq |s| \int_n^t x^{-\mathrm{Re}(s)-1}\,\mathrm{d}x \leq |s| n^{-\mathrm{Re}(s)-1},$$

with the last quantity in the previous display independent of t and having the power of n smaller by 1. It follows that

$$\left| \int_n^{n+1} (n^{-s} - t^{-s})\,\mathrm{d}t \right| \leq |s| n^{-\mathrm{Re}(s)-1}.$$

This estimate shows that the sum

$$\psi(s) = \sum_{n=1}^{\infty} \int_n^{n+1} (n^{-s} - t^{-s})\,\mathrm{d}t$$

converges on $\{s : \mathrm{Re}(s) > 0\}$, uniformly on compact subsets, making $\psi(s)$ analytic there. Thus

$$\zeta(s) = \psi(s) + \frac{1}{s-1}, \quad \mathrm{Re}(s) > 1.$$

But the right side is meromorphic for $\mathrm{Re}(s) > 0$, its only singularity for such s being a simple pole at $s = 1$ with residue 1. The previous display extends ζ and gives it the same properties.

The value $\psi(1) = \lim_{s\to 1}(\zeta(s) - \frac{1}{s-1})$ is called *Euler's constant* and denoted γ,

$$\zeta(s) = \frac{1}{s-1} + \gamma + \mathcal{O}(s-1), \qquad \gamma = \sum_{n=1}^{\infty} \int_n^{n+1} (n^{-1} - t^{-1})\,\mathrm{d}t.$$

With H_N denoting the Nth harmonic number $\sum_{n=1}^{N} n^{-1}$, Euler's constant is

$$\gamma = \lim_{N\to\infty} (H_N - \log N).$$

As above, this is the area above the $y = 1/x$ curve for $x \geq 1$ but inside the circumscribing boxes $[n, n+1] \times [0, 1/n]$ for $n \geq 1$.

One way to extend $L(\chi, s)$ to $\mathrm{Re}(s) > 0$ for $\chi \neq 1$ uses the discrete analogue of integration by parts.

Proposition 11.1 (Summation by Parts)**.** *Let $\{a_n\}_{n\geq 1}$ and $\{b_n\}_{n\geq 1}$ be complex sequences. Define*

$$A_n = \sum_{k=1}^{n} a_k \quad \textit{for } n \geq 0 \ (\textit{including } A_0 = 0),$$

so that

$$a_n = A_n - A_{n-1} \quad \textit{for } n \geq 1.$$

Also define

$$\Delta b_n = b_{n+1} - b_n \quad \textit{for } n \geq 1.$$

Then for any $1 \leq m \leq n$, the summation by parts formula is

$$\sum_{k=m}^{n-1} a_k b_k = A_{n-1} b_n - A_{m-1} b_m - \sum_{k=m}^{n-1} A_k \Delta b_k.$$

Proof. The formula is easy to verify in consequence of

$$a_k b_k = A_k b_{k+1} - A_{k-1} b_k - A_k \Delta b_k, \quad k \geq 1,$$

noting that the first two terms on the right side telescope when summed. □

For example, the proposition shows that $\sum_{k=1}^{\infty} k e^{-k} = e/(e-1)^2$.

Returning to $L(\chi, s) = \sum_{n\in\mathbb{Z}^+} \chi(n) n^{-s}$ where χ is nontrivial, the first orthogonality relation gives

$$\sum_{n=n_0}^{n_0+N-1} \chi(n) = 0 \quad \text{for any } n_0 \in \mathbb{Z}^+.$$

Let $\{a_n\} = \{\chi(n)\}$ and $\{b_n\} = \{n^{-s}\}$, and note that $\{A_n\}$ is bounded while $|\Delta b_n| \leq |s| n^{-\mathrm{Re}(s)-1}$ as shown above. Summation by parts gives

$$L(\chi, s) = \lim_n \sum_{k=1}^{n-1} a_k b_k = -\lim_n \sum_{k=1}^{n-1} A_k \Delta b_k,$$

and the right side converges on $\{s : \mathrm{Re}(s) > 0\}$, uniformly on compacta. Thus $L(\chi, s)$ is analytic on $\{s : \mathrm{Re}(s) > 0\}$.

Summation by parts gives a second argument for the continuation of the zeta function as well. For any prime q, introduce the sequence of coefficients $\{a_n\}$ consisting of $q-1$ times 1, then a single $1-q$, then $q-1$ more times 1, then another $1-q$, and so on,

$$\{a_n\} = \{1, 1, \dots, 1, 1-q, 1, 1, \dots, 1, 1-q, 1, 1, \dots, 1, 1-q, \dots\}.$$

and consider the Dirichlet series

$$f_q(s) = \sum_{n \geq 1} a_n n^{-s}.$$

The sequence of partial sums of the coefficients is (starting at index 0 here)

$$\{A_n\} = \{0, 1, 2, \dots, q-1, 0, 1, 2, \dots, q-1, 0, 1, 2, \dots, q-1, 0, \dots\}.$$

And so summation by parts shows that the Dirichlet series $f_q(s)$ is analytic on $\mathrm{Re}(s) > 0$.

Compute that for $\mathrm{Re}(s) > 1$ (where we have absolute convergence and therefore may rearrange terms freely),

$$f_q(s) = \sum_{n \geq 1} n^{-s} - q \sum_{n \geq 1} (qn)^{-s} = (1 - q^{1-s})\zeta(s), \quad \mathrm{Re}(s) > 1.$$

Because $f_q(s)$ is analytic on $\{\mathrm{Re}(s) > 0\}$ and agrees with $(1-q^{1-s})\zeta(s)$ on $\{\mathrm{Re}(s) > 1\}$, it follows that $(1-q^{1-s})\zeta(s)$ continues analytically to $\{\mathrm{Re}(s) > 0\}$. Therefore $\zeta(s)$ continues meromorphically to $\{\mathrm{Re}(s) > 0\}$ with poles possible only where $q^{1-s} = 1$.

Because $q^{1-s} = e^{(1-s)\ln q}$, the condition $q^{1-s} = 1$ is $s \in 1 + 2\pi i \mathbb{Z}/\ln q$. Thus the only possible poles of $\zeta(s)$ in $\{\mathrm{Re}(s) > 0\}$ are distributed evenly along the line $\mathrm{Re}(s) = 1$ with spacing $2\pi/\ln q$. However, the prime q is arbitrary, and the sets $2\pi\mathbb{Z}/\ln q$ and $2\pi\mathbb{Z}/\ln q'$ for distinct primes q and q' meet only at 0. Thus the only possible pole of the extended $\zeta(s)$ is at $s = 1$. This completes the proof.