

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. And furthermore, for fixed N the primes distribute evenly among the arithmetic progressions corresponding to different values of a .

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

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

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.

2. EULER'S PROOF OF INFINITELY MANY PRIMES

Recall some formulas:

- Geometric series:

$$\sum_{\nu=0}^{\infty} X^{\nu} = (1 - X)^{-1}, \quad X \in \mathbb{C}, |X| < 1,$$

- Logarithm series:

$$\log(1 - X)^{-1} = \sum_{\nu=1}^{\infty} \nu^{-1} X^{\nu}, \quad X \in \mathbb{C}, |X| < 1,$$

- Telescoping series:

$$\sum_{\nu=2}^{\infty} \frac{1}{\nu(\nu-1)} = 1.$$

(Proof: $\frac{1}{\nu(\nu-1)} = \frac{1}{\nu-1} - \frac{1}{\nu}$.)

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:

$$\begin{aligned} \sum_{n=2^e} n^{-s} &= \sum_{e=0}^{\infty} (2^{-s})^e = (1 - 2^{-s})^{-1}, \\ \sum_{n=2^{e_1} 3^{e_2}} n^{-s} &= \sum_{e_1=0}^{\infty} (2^{-s})^{e_1} \sum_{e_2=0}^{\infty} (3^{-s})^{e_2} = (1 - 2^{-s})^{-1} (1 - 3^{-s})^{-1}, \\ &\vdots \\ \sum_{n=2^{e_1} \dots p_r^{e_r}} n^{-s} &= \prod_{i=1}^r \sum_{e_i=0}^{\infty} (p_i^{-s})^{e_i} = \prod_{i=1}^r (1 - p_i^{-s})^{-1}, \\ &\vdots \\ \sum_{n \in \mathbb{Z}^+} n^{-s} &= \prod_{p \in \mathcal{P}} (1 - p^{-s})^{-1}. \end{aligned}$$

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 ,

$$\log \zeta(s) = \log \prod_{p \in \mathcal{P}} (1 - p^{-s})^{-1} = \sum_{p \in \mathcal{P}} \log(1 - p^{-s})^{-1} = \sum_{p \in \mathcal{P}} \sum_{\nu=1}^{\infty} \nu^{-1} p^{-\nu s}.$$

That is,

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

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,

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

And so

$$\log \zeta(s) - 1 < \sum_{p \in \mathcal{P}} p^{-s} < \log \zeta(s).$$

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

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

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 . It is fairly easy to show that $G^* \cong G$, 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 $\chi(g) \neq 1_{\mathbb{C}}$.

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

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

and then the *Fourier series* of f is

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

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

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

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 to pick off $a \pmod{N}$,

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

Then for any $\chi \in G^*$, the χ th Fourier coefficient of f is simply

$$\widehat{f}(\chi) = \chi(a^{-1})/\phi(N),$$

and the relation $s_f(x) = f(x)$ 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 $\sum_{p=a(N)} p^{-s}$. The indicator function f lets us take the sum over all primes instead and then replace f by its Fourier series $s_f = (1/\phi(N)) \sum_{\chi} \chi(a^{-1}) \chi$ to get

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

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

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

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 extended 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 extend 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 $(\mathbb{Z}/1\mathbb{Z})^\times = \{\bar{0}\}$. The primitive trivial character lifts to the constant function $1(n) = 1$ for all $n \in \mathbb{Z}$.

5. 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 $\chi : \mathbb{Z} \rightarrow \mathbb{C}$) define

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

(Equality of the sum and product follow from a straightforward analogue to the proof of Euler's identity, since characters are homomorphisms.) Then

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

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

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

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 previous two displays 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,

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

Now the goal is to show that the right side goes to $+\infty$ as $s \rightarrow 1^+$. 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*.

6. ANALYTIC PROPERTIES OF $L(\chi, s)$

We need to study the behavior of $L(\chi, s)$ as $s \rightarrow 1^+$. 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

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

Here $n^{-s} = e^{-s \ln n}$ for $n \in \mathbb{Z}^+$. The sum expression for $L(\chi, s)$ converges absolutely on the half plane $\{s : \operatorname{Re}(s) > 1\}$, 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 6.1. *The function $L(\chi, s)$ has a meromorphic continuation to the right half plane $\{\operatorname{Re}(s) > 0\}$. If $\chi = 1$ then the extended function $\zeta(s)$ has a simple pole at $s = 1$ with residue 1. 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, but such arguments do not scale up beyond the situation at hand. In a separate writeup, results that subsume the proposition are proved by methods that have scope.

We reiterate here that the identity

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

meaning that

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

is the substance of Euler's proof.

7. THE SECOND IDEA OF DIRICHLET'S PROOF

Recall that for $s > 1$,

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

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

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

and Dirichlet's proof is complete.

So we need to study the function

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

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

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

or

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

We must 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 $\zeta_N(s)$ as the cyclotomic Dedekind zeta function, but in doing so it must invoke some language and some results from algebraic number theory.

8. MEROMORPHY OF $\zeta_N(s)$ AT $s = 1$

Lemma 8.1. *Let p be prime. Let $N = p^d N_p$ with $p \nmid N_p$. Let f be the order of p in $(\mathbb{Z}/N_p\mathbb{Z})^\times$, i.e., the smallest positive integer such that $p^f \equiv 1 \pmod{N_p}$. Let $g = \phi(N_p)/f$. Then for any indeterminate T ,*

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

(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 extended M -periodically to $\chi : \mathbb{Z} \rightarrow \mathbb{C}$, which is evaluated at p . When $p \nmid N$ the whole process merely reproduces $\chi(p + N\mathbb{Z})$, now referring to the original χ . 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 on the left side of the lemma's equality is nontrivial if and only if the original χ descends to a character—not necessarily primitive—modulo N_p . Any character in G^* that does not descend to a character modulo N_p is irrelevant to the lemma's equality.

A character χ modulo N_p takes p to 1 if and only if it factors through the quotient group $(\mathbb{Z}/N_p\mathbb{Z})^\times / \langle p + N_p\mathbb{Z} \rangle$. This quotient group has order $\phi(N_p)/f = g$, and so it has g characters. That is, g characters χ modulo N_p take p to 1. Also, for each $j \in \{0, 1, \dots, f-1\}$ there exist characters χ modulo N_p that take p to ρ^j where ρ is a primitive complex f th root of unity. Thus for each such j there exist g characters χ modulo N_p that take p to ρ^j , independently of k . And as already mentioned, every character modulo N that is not defined modulo N_p takes p to 0.

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

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

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

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

□

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 fussing about it holding for G^* . Our reason for insisting on G^* is manifest in the proof of the next proposition.

Proposition 8.2. $\zeta_N(s) = \prod_{p \in \mathcal{P}} (1 - p^{-fs})^{-g}$ for $\operatorname{Re}(s) > 1$.

Proof. Compute, using the lemma at the last step,

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

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

Theorem 8.3. $\zeta_N(s)$ 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 $\{s : \operatorname{Re}(s) > 0\}$ so that its product expression converges there. But for $s \in \mathbb{R}^+$,

$$(1 - p^{-fs})^{-g} = \left(\sum_{\nu=0}^{\infty} p^{-\nu fs} \right)^g \geq \sum_{\nu=0}^{\infty} p^{-\nu \phi(N)s} = (1 - p^{-\phi(N)s})^{-1},$$

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. \square

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

9. REVIEW OF THE PROOFS

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

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

The corresponding ideas in Dirichlet's proof were

$$\begin{aligned} L(\chi, s) &= \sum_{n \in \mathbb{Z}^+} \chi(n) n^{-s} = \prod_{p \in \mathcal{P}} (1 - \chi(p) p^{-s})^{-1}, \\ \sum_{\substack{p \in \mathcal{P} \\ p \equiv a(N)}} p^{-s} &\sim \frac{1}{\phi(N)} \sum_{\chi \in G^*} \chi(a)^{-1} \log L(\chi, s), \\ \lim_{s \rightarrow 1} \zeta_N(s) &= \infty \quad \text{where } \zeta_N(s) = \prod_{\chi \in G^*} L(\chi, s). \end{aligned}$$

Consequently,

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

In other words,

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

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 $a + N\mathbb{Z}$.

10. PLACE-HOLDER CONTINUATION ARGUMENTS

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

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

This last sum is an infinite sum of analytic functions; call it $-\psi(s)$. Since for all $t \in [n, n+1]$ we have

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

it follows that

$$\left| \int_n^{n+1} (t^{-s} - n^{-s}) dt \right| \leq \frac{|s|}{n^{\operatorname{Re}(s)+1}},$$

and so the sum $-\psi(s)$ converges on $\{s : \operatorname{Re}(s) > 0\}$, uniformly on compact subsets, making $\psi(s)$ analytic there. Thus

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

But the right side is meromorphic for $\operatorname{Re}(s) > 0$, 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.

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

Proposition 10.1 (Summation by Parts). *Let $\{a_n\}_{n \geq 1}$ and $\{b_n\}_{n \geq 1}$ be complex sequences. Define*

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

so that

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

Also define

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

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

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

□

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

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

Let $\{a_n\} = \{\chi(n)\}$ and $\{b_n\} = \{n^{-s}\}$, and note that $\{A_n\}$ is bounded while $\Delta b_n \sim n^{-\operatorname{Re}(s)-1}$. 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 $\{s : \operatorname{Re}(s) > 0\}$, uniformly on compacta. Thus $L(\chi, s)$ is analytic on $\{s : \operatorname{Re}(s) > 0\}$.

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 $\operatorname{Re}(s) > 0$.

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

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

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

The condition $q^{1-s} = 1$ readily works out to $s \in 1 + 2\pi i\mathbb{Z}/\ln q$. Thus the only possible poles of $\zeta(s)$ in $\{\operatorname{Re}(s) > 0\}$ are distributed evenly along the line $\operatorname{Re}(s) = 1$ with spacing $2\pi/\ln q$. However, q is arbitrary, and a small exercise shows that the sets $2\pi\mathbb{Z}/\ln q$ and $2\pi\mathbb{Z}/\ln q'$ meet only at 0 for distinct primes q and q' . Thus the only possible pole of the extended $\zeta(s)$ is at $s = 1$. This completes the proof.