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
\[
\{a, a + N, a + 2N, a + 3N, \ldots \}
\]
contain infinitely many primes?

For example, if $a = 4$, $N = 15$, does the arithmetic progression
\[
\{4, 19, 34, 49, \ldots \}
\]
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:

\[
\begin{align*}
\{1, 1 + 15, 1 + 2 \times 15, 1 + 3 \times 15, \ldots \}, \\
\{2, 2 + 15, 2 + 2 \times 15, 2 + 3 \times 15, \ldots \}, \\
\{4, 4 + 15, 4 + 2 \times 15, 4 + 3 \times 15, \ldots \}, \\
\{7, 7 + 15, 7 + 2 \times 15, 7 + 3 \times 15, \ldots \}, \\
\{8, 8 + 15, 8 + 2 \times 15, 8 + 3 \times 15, \ldots \}, \\
\{11, 11 + 15, 11 + 2 \times 15, 11 + 3 \times 15, \ldots \}, \\
\{13, 13 + 15, 13 + 2 \times 15, 13 + 3 \times 15, \ldots \}, \\
\{14, 14 + 15, 14 + 2 \times 15, 14 + 3 \times 15, \ldots \}.
\end{align*}
\]

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 \( n = p_1^{e_1}p_2^{e_2} \cdots p_r^{e_r} \) with all \( e_i \in \mathbb{N} \) and almost all \( e_i = 0 \). Euler’s identity really just rephrases this fact:
  \[
  \sum_{n = 2^s} n^{-s} = \sum_{c=0}^{\infty} (2^{-s})^c = (1 - 2^{-s})^{-1},
  \]
  \[
  \sum_{n = 2^s \times 3^e} n^{-s} = \sum_{c_1=0}^{\infty} (2^{-s})^{c_1} \sum_{c_2=0}^{\infty} (3^{-s})^{c_2} = (1 - 2^{-s})^{-1}(1 - 3^{-s})^{-1},
  \]
  \[
  \vdots
  \]
  \[
  \sum_{n = 2^{s_1} \cdots p_r^{s_r}} n^{-s} = \prod_{i=1}^{r} \sum_{c_i=0}^{\infty} (p_i^{-s})^{c_i} = \prod_{i=1}^{r} (1 - p_i^{-s})^{-1},
  \]
  \[
  \vdots
  \]
  \[
  \sum_{n \in \mathbb{Z}^+} n^{-s} = \prod_{p \in \mathcal{P}} (1 - p^{-s})^{-1}.
  \]

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

  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 $\zeta$, $\lim_{s \to 1^+} \zeta(s) = \infty$ 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’s idea was to modify Euler’s proof by introducing additional factors in $\zeta(s)$ to pick off only primes $p$ such that $p \equiv a \pmod{N}$.

Let $G = (\mathbb{Z}/N\mathbb{Z})^\times$, a finite abelian multiplicative group of order $|G| = \phi(N)$ where $\phi$ is Euler’s totient function.

Define
\[
G^* = \{ \text{homomorphisms} : G \to \mathbb{C}^\times \}.
\]
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 $\chi$ 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 any function $f : G \to \mathbb{C}$, the Fourier transform of $f$ is a corresponding function on the dual group,
\[
\hat{f} : G^* \to \mathbb{C}, \quad \hat{f}(\chi) = \frac{1}{\phi(N)} \sum_{x \in G} f(x) \chi(x^{-1}),
\]
and then the Fourier series of $f$ is
\[
s_f : G \to \mathbb{C}, \quad s_f = \sum_{\chi \in G^*} \hat{f}(\chi) \chi.
\]
The second orthogonality relation shows that the Fourier series reproduces the original function,
\[
s_f(x) = \frac{1}{\phi(N)} \sum_{\chi \in G^*} \sum_{y \in G} f(y) \chi(xy^{-1})
\]
\[
= \frac{1}{\phi(N)} \sum_{y \in G} f(y) \sum_{\chi \in G^*} \chi(xy^{-1}) = f(x).
\]
No qualifications on the function $f$, and no convergence issues of any sort, are involved here since the group $G$ is finite.

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 $\chi$th Fourier coefficient of $f$ is simply

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

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

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

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 $\chi$, as follows. First, there exists a least positive divisor $M$ of $N$ such that $\chi$ factors as

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

The integer $M$ is the conductor of $\chi$, and the character $\chi_o$ 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 $\chi$ to denote the primitive character $\chi_o$ 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 $\chi$ on the left and the original $\chi$ on the right,

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

justifies the multiple use of the symbol $\chi$. (For example, the orthogonality relations are undisturbed if we apply the new $\chi$ to coset representatives rather than applying the original $\chi$ 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 $\chi_o$ 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 $1$.
5. \textbf{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
$$\{p \in \mathbb{P} : p \equiv a \pmod{N}\}$$
is infinite.

For each $\chi \in G^\times$ (with its corresponding $\chi : \mathbb{Z} \to \mathbb{C}$) define
$$L(s, \chi) = \sum_{n \in \mathbb{Z}^+} \chi(n)n^{-s} = \prod_{p \in \mathbb{P}} \left( 1 - \chi(p)p^{-s} \right)^{-1}, \quad s > 1.$$ (Equality of the sum and product follow from a straightforward analogue to the proof of Euler’s identity, since characters are homomorphisms.) Then
$$\log L(s, \chi) = \sum_{p \in \mathbb{P}} \nu^{-1} \chi(p^\nu)p^{-\nu s} = \sum_{p \in \mathbb{P}} \chi(p)p^{-s} + \sum_{p \in \mathbb{P}, \nu \geq 2} \nu^{-1} \chi(p^\nu)p^{-\nu s},$$
and the second term has absolute value at most 1 by the argument in Euler’s proof.

Recall the formula that came from the Fourier series of the indicator function of $a \pmod{N}$,
$$\sum_{p=a(N)} p^{-s} = \frac{1}{\varphi(N)} \sum_{\chi} \chi(a^{-1}) \sum_{p \in \mathbb{P}} \chi(p)p^{-s}.$$ The previous two displays show that the linear combination of \{log $L(s, \chi)$\} whose coefficients are the Fourier coefficients of the indicator function is the desired sum plus a small error term,
$$\frac{1}{\varphi(N)} \sum_{\chi} \chi(a^{-1}) \log L(s, \chi) = \sum_{p=a(N)} p^{-s} + \varepsilon, \quad |\varepsilon| < 1.$$ Now the goal is to show that the left 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 $L(s, \chi)$ for nontrivial $\chi$ sensibly takes a finite but nonzero value.

6. Properties of $\zeta(s)$

We need to study the behavior of $L(s, \chi)$ as $s \to 1^+$. Even though $s$ is real, $L(s, \chi)$ 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 $\zeta$ to
$$\zeta(s) = \sum_{n \in \mathbb{Z}^+} n^{-s} = \prod_{p \in \mathbb{P}} (1 - p^{-s})^{-1}, \quad s \in \mathbb{C}, \ \text{Re}(s) > 1.$$ (Here $n^{-s} = e^{-s \ln n}$ for $n \in \mathbb{Z}^+$.)

\textbf{Proposition 6.1.} The zeta function $\zeta(s)$ has the following properties.

(a) It is analytic on the right half plane \{s : \text{Re}(s) > 1\}.

(b) It has a meromorphic extension to the right half plane \{s : \text{Re}(s) > 0\}, and the extension is analytic other than a simple pole at $s = 1$ with residue 1. That is,
$$\zeta(s) = \frac{1}{s-1} + \psi(s), \quad s \in \mathbb{C}, \ \text{Re}(s) > 0$$where $\psi$ is analytic.
(c) Its logarithm satisfies the asymptotic relation
\[ \log \zeta(s) \sim \sum_{p \in \mathcal{P}} p^{-s}, \]
meaning that
\[ \lim_{s \to 1^+} \frac{\log \zeta(s)}{\sum_{p \in \mathcal{P}} p^{-s}} = 1. \]

Proof. (a) The sum expression for \( \zeta(s) \) converges on the half plane \( \{ s : \text{Re}(s) > 1 \} \), and the convergence is uniform on compacta. Its summands, hence its partial sums, are analytic. So \( \zeta(s) \) is analytic on the half plane.

(b) Compute that
\[ \frac{1}{s-1} = \int_1^{\infty} t^{-s} dt = \sum_{n=1}^{\infty} \int_n^{n+1} t^{-s} dt = \zeta(s) + \sum_{n=1}^{\infty} \int_n^{n+1} (t^{-s} - n^{-s}) dt. \]
This last sum is an infinite sum of analytic functions; call it \( -\psi(s) \). Since for all \( t \in [n, n+1] \) we have
\[ |t^{-s} - n^{-s}| = |s| \int_n^t x^{-s-1} dx \leq |s| \int_n^t x^{-\text{Re}(s)-1} dx \leq |s| n^{-\text{Re}(s)-1}, \]
it follows that
\[ \left| \int_n^{n+1} (t^{-s} - n^{-s}) dt \right| \leq \frac{|s|}{n^{\text{Re}(s)+1}}, \]
and so the sum \( -\psi(s) \) converges on \( \{ s : \text{Re}(s) > 0 \} \), uniformly on compact subsets, making \( \psi(s) \) analytic there.

(c) This is the substance of Euler’s proof. \( \square \)

7. Properties of \( L(s, \chi) \)

As with the zeta function, we want to extend the domain of \( L(s, \chi) \) to complex values of \( s \) and then bring complex analysis to bear on its behavior.

First consider the case \( \chi = 1 \). The function on \( \mathbb{Z} \) corresponding to this character is identically 1. Thus
\[ L(s, 1) = \zeta(s). \]
That is, \( L(s, 1) \) is meromorphic on \( \{ s : \text{Re}(s) > 0 \} \) with a simple pole at \( s = 1 \) and no other poles.

Now consider the case \( \chi \neq 1 \). By the first orthogonality relation,
\[ \sum_{n=n_0}^{n_0+N} \chi(n) = 0 \quad \text{for any } n_0 \in \mathbb{Z}^+, \]
and it follows by a technique called partial summation (the discrete analogue of integration by parts) that \( L(s, \chi) = \sum_{n \in \mathbb{Z}^+} \chi(n)n^{-s} \) converges on \( \{ s : \text{Re}(s) > 0 \} \), uniformly on compacta. Thus \( L(s, \chi) \) is analytic on \( \{ s : \text{Re}(s) > 0 \} \).
8. The second idea of Dirichlet’s proof

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

Also, \( L(s, 1) \to \infty \) as \( s \to 1 \). We will show that for \( \chi \neq 1 \), \( L(1, \chi) \neq 0 \) and thus \( \log L(1, \chi) \) is finite. Since \( |\chi(a)^{-1}| = 1 \) for all \( \chi \in G^* \), it follows that
\[
\lim_{s \to 1^+} \left| \sum_{\chi \in G^*} \chi(a)^{-1} \log L(s, \chi) \right| = +\infty
\]
and Dirichlet’s proof is complete.

So we need to study the function
\[
\zeta_N(s) = \prod_{\chi \in G^*} L(s, \chi).
\]

Since \( L(s, 1) \) is meromorphic on \( \{ s : \text{Re}(s) > 0 \} \) with a simple pole at \( s = 1 \) and all other \( L(s, \chi) \) are analytic on \( \{ s : \text{Re}(s) > 0 \} \), there are two possibilities. Either
\[
\zeta_N(s) \text{ is meromorphic on } \{ s : \text{Re}(s) > 0 \} \text{ with a simple pole at } s = 1
\]
or
\[
\zeta_N(s) \text{ is analytic on } \{ s : \text{Re}(s) > 0 \}.
\]
We must rule out the second possibility to complete the proof.

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 \( f \) 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, \( \chi(p) \) denotes an original \( \chi \in G^* \), reduced to a primitive \( \chi_o : (\mathbb{Z}/M\mathbb{Z})^\times \to \mathbb{C}^\times \) where \( M \mid N \) is the conductor, then extended to \( \chi : \mathbb{Z} \to \mathbb{C} \), and finally evaluated at \( p \). When \( p \nmid N \) the whole process merely reproduces \( \chi(p + N\mathbb{Z}) \), now referring to the original \( \chi \). In general, \( \chi(p) \) in the lemma’s formula is nonzero if and only if \( p \) does not divide the conductor \( M \) of the original \( \chi \), i.e., \( \chi(p) \neq 0 \) if and only if the original \( \chi \) descends to a character—not necessarily primitive—modulo \( N_p \). The decomposition \( (\mathbb{Z}/N_p\mathbb{Z})^\times = (p + N_p\mathbb{Z}) \times Q \), where \( |(p + N_p\mathbb{Z})| = f \) and \( |Q| = g \), shows that of the \( \phi(N_p) = fg \) such characters, \( g \) take \( p \) to \( 1 \), \( g \) take \( p \) to \( e^{2\pi i/f} \), \( g \) take \( p \) to \( e^{4\pi i/f} \), and so on. The characters in \( G^* \) such that \( p \) does divide the conductor contribute multiplicands of \( 1 \) to the product in the lemma, i.e., they are irrelevant to the formula.
Proof. Let \( \rho \) 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

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

since for each \( j \), \( g \) is the number of characters \( \chi \in G^* \) such that \( \chi(p) = \rho^j \).

The reader may note that in the lemma we could have let \( H = (\mathbb{Z}/N\mathbb{Z})^\times \) (which is \( (\mathbb{Z}/\mathbb{Z})^\times = G \) for all \( p \nmid N \)) and then stated the lemma’s formula using a product over \( \chi \in H^* \) rather than go through all the fussing with \( G^* \). The reason for insisting on \( G^* \) is manifest in the proof of the next proposition.

**Proposition 9.2.** \( \zeta_N(s) = \prod_{p \in \mathcal{P}} (1 - p^{-fs})^{-g} \).

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

\[
\zeta_N(s) = \prod_{\chi \in G^*} L(s, \chi) = \prod_{\chi \in G^*} \prod_{p \in \mathcal{P}} (1 - \chi(p)p^{-s})^{-1}
\]

\[
= \prod_{p \in \mathcal{P}} \prod_{\chi \in G^*} (1 - \chi(p)p^{-s})^{-1} = \prod_{p \in \mathcal{P}} (1 - p^{-fs})^{-g}.
\]

\[\square\]

**Theorem 9.3.** \( \zeta_N(s) \) has a simple pole at \( s = 1 \).

**Proof.** The only other possibility is that \( \zeta_N(s) \) is analytic on \( \{ s : \text{Re}(s) > 0 \} \) so that its product expression converges there. But for \( s \in \mathbb{R}^+ \),

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

and so for \( s \in \mathbb{R}^+ \),

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

but \( \zeta(\phi(N)s) \) diverges at \( s = 1/\phi(N) \), giving a contradiction. \[\square\]

**Corollary 9.4.** For \( \chi \neq 1 \), \( L(1, \chi) \) is finite and nonzero.

It deserves passing mention that \( \zeta_N(s) \) has another, more natural definition as the **cyclotomic Dedekind zeta function**. Describing the cyclotomic Dedekind zeta function requires language beyond our scope, but granted the definition, one uses cyclotomic arithmetic to reverse the calculation here, again obtaining the factorization

\[
\zeta_N(s) = \prod_p (1 - p^{-fs})^{-g} = \prod_{\chi \in G^*} L(s, \chi)
\]

of \( \zeta_N(s) \) as the product of the Dirichlet \( L \)-functions as a theorem rather than a definition.
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

\[
\zeta(s) = \sum_{n \in \mathbb{Z}^+} n^{-s} = \prod_{p \in \mathcal{P}} (1 - p^{-s})^{-1},
\]

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

\[
\lim_{s \to 1^+} \zeta(s) = \infty.
\]

The corresponding ideas in Dirichlet’s proof were

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

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

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

Consequently,

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

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 \( \{ p \in \mathcal{P} : p \equiv a \pmod{N} \} \) finite, 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 \( a + N\mathbb{Z} \).