

## 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:

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

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:

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

- Logarithm series:

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

- 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):

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

The Fundamental Theorem of Arithmetic asserts that any  $n \in \mathbf{Z}^+$  is uniquely expressible as  $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r} \dots$  with all  $e_i \in \mathbf{N}$  and almost all  $e_i = 0$ . Euler's identity really just rephrases this fact:

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

With Euler's identity in place, his proof that there are infinitely many primes follows. Let

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

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,

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

so

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

By the sum expansion of  $\zeta$ ,  $\lim_{s \rightarrow 1^+} \zeta(s) = \infty$  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'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  $G = (\mathbf{Z}/N\mathbf{Z})^\times$ , a finite abelian multiplicative group of order

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

Define

$$\begin{aligned} G^* &= \{\text{homomorphisms } : G \longrightarrow \mathbf{C}^\times\} \\ &= \{\chi : G \longrightarrow \mathbf{C}^\times \mid \chi(g_1 g_2) = \chi(g_1) \chi(g_2) \text{ for all } g_1, g_2 \in G\}. \end{aligned}$$

Then  $G^*$  forms a finite abelian multiplicative group also. Specifically, for  $\chi_1, \chi_2 \in G^*$ , 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. And the following pretty, useful formulas hold.

**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  $g \in G$ ,

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

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

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

The integer  $M$  is the *conductor* of  $\chi$ , and the character  $\chi_o$  is *primitive*. Note that

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

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

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

The following relation, with the new  $\chi$  on the left and the original  $\chi$  on the right,

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

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  $\chi(n + N\mathbf{Z})$  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 on  $(\mathbf{Z}/1\mathbf{Z})^\times = \{\bar{0}\}$ . The primitive trivial character lifts to the constant function  $1(n) = 1$  for all  $n \in \mathbf{Z}$ .

#### 4. L-FUNCTIONS AND THE FIRST IDEA OF DIRICHLET'S PROOF

Recall that  $G = (\mathbf{Z}/N\mathbf{Z})^\times$ ,  $a \in G$ , 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  $\chi : \mathbf{Z} \rightarrow \mathbf{C}$ ) define

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

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

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

Multiply through by  $\chi(a)^{-1}$  and sum over all  $\chi \in G^*$  to get

$$\sum_{\chi \in G^*} \chi(a)^{-1} \log L(s, \chi) = \sum_{p \in \mathcal{P}} \sum_{\nu=1}^{\infty} \nu^{-1} p^{-\nu s} \sum_{\chi \in G^*} \chi(a^{-1} p^\nu).$$

(Here  $a^{-1}$  denotes the inverse of  $a + N\mathbf{Z}$  in  $G = (\mathbf{Z}/N\mathbf{Z})^\times$ .) By the second orthogonality relation,

$$\sum_{\chi \in G^*} \chi(a^{-1} p^\nu) = \begin{cases} |G^*| & \text{if } p^\nu \equiv a \pmod{N}, \\ 0 & \text{otherwise.} \end{cases}$$

So, since  $|G^*| = \phi(N)$ ,

$$\begin{aligned} \frac{1}{\phi(N)} \sum_{\chi \in G^*} \chi(a)^{-1} \log L(s, \chi) &= \sum_{p \in \mathcal{P}} \sum_{\substack{\nu=1 \\ p^\nu \equiv a(N)}}^{\infty} \nu^{-1} p^{-\nu s} \\ &= \sum_{\substack{p \in \mathcal{P} \\ p \equiv a(N)}} p^{-s} + \sum_{p \in \mathcal{P}} \sum_{\substack{\nu=2 \\ p^\nu \equiv a(N)}}^{\infty} \nu^{-1} p^{-\nu s} \\ &< \sum_{\substack{p \in \mathcal{P} \\ p \equiv a(N)}} p^{-s} + 1. \end{aligned}$$

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

### 5. PROPERTIES OF $\zeta(s)$

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

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

(Here  $n^{-s} = e^{-s \ln n}$  for  $n \in \mathbf{Z}^+$ .)

**Proposition 5.1.** *The zeta function  $\zeta(s)$  has the following properties.*

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

(b) *It has a meromorphic extension to the right half plane  $\{s : \operatorname{Re}(s) > 0\}$ , and the extension is analytic other than a simple pole at  $s = 1$  with residue 1. That is,*

$$\zeta(s) = \frac{1}{s-1} + \psi(s), \quad s \in \mathbf{C}, \operatorname{Re}(s) > 0$$

where  $\psi$  is analytic.

(c) *Its logarithm satisfies the asymptotic relation*

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

meaning that

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

*Proof.* (a) The sum expression for  $\zeta(s)$  converges on the half plane  $\{s : \operatorname{Re}(s) > 1\}$ , 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

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

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.

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

6. 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  $\mathbf{Z}$  corresponding to this character is identically 1. Thus

$$L(s, 1) = \zeta(s).$$

That is,  $L(s, 1)$  is meromorphic on  $\{s : \operatorname{Re}(s) > 0\}$  with a simple pole at  $s = 1$  and no other poles.

Now consider the case  $\chi \neq 1$ . By the first orthogonality relation,

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

and it follows by a technique called partial summation (the discrete analogue of integration by parts) that  $L(s, \chi) = \sum_{n \in \mathbf{Z}^+} \chi(n)n^{-s}$  converges on  $\{s : \operatorname{Re}(s) > 0\}$ , uniformly on compacta. Thus  $L(s, \chi)$  is analytic on  $\{s : \operatorname{Re}(s) > 0\}$ .

## 7. 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,  $L(s, 1) \rightarrow \infty$  as  $s \rightarrow 1$ . 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

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

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  $\{s : \operatorname{Re}(s) > 0\}$  with a simple pole at  $s = 1$  and all other  $L(s, \chi)$  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.

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  $(\mathbf{Z}/N_p \mathbf{Z})^\times$ , 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  $\chi_o : (\mathbf{Z}/M\mathbf{Z})^\times \rightarrow \mathbf{C}^\times$  where  $M \mid N$  is the conductor, then extended to  $\chi : \mathbf{Z} \rightarrow \mathbf{C}$ , and finally evaluated at  $p$ . When  $p \nmid N$  the whole process merely reproduces  $\chi(p + N\mathbf{Z})$ , 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  $(\mathbf{Z}/N_p \mathbf{Z})^\times = \langle p + N_p \mathbf{Z} \rangle \times Q$ , where  $|\langle p + N_p \mathbf{Z} \rangle| = f$  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  $f^{\text{th}}$  root of unity in  $\mathbf{C}$ . 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  $\chi(p) = \rho^j$ .  $\square$

The reader may note that in the lemma we could have let  $H = (\mathbf{Z}/N_p \mathbf{Z})^\times$  (which is  $(\mathbf{Z}/N\mathbf{Z})^\times = G$  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 8.2.**  $\zeta_N(s) = \prod_{p \in \mathcal{P}} (1 - p^{-fs})^{-g}$ .

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

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

$\square$

**Theorem 8.3.**  $\zeta_N(s)$  has a simple pole at  $s = 1$ .

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

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

and so for  $s \in \mathbf{R}^+$ ,

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

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

**Corollary 8.4.** *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.

## 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

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

The corresponding ideas in Dirichlet's proof were

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

Consequently,

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

In other words,

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

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  $a + N\mathbf{Z}$ .