THE REVIEW OF SYMBOLIC LOGIC
Volume 9, Number 3, September 2016

CHARACTER AND OBJECT

JEREMY AVIGAD AND REBECCA MORRIS

Abstract. In 1837, Dirichlet proved that there are infinitely many primes in any arithmetic progression in which the terms do not all share a common factor. Modern presentations of the proof are explicitly of higher-order, in that they involve quantifying over and summing over *Dirichlet characters*, which are certain types of functions. The notion of a character is only implicit in Dirichlet's original proof, and the subsequent history shows a very gradual transition to the modern mode of presentation.

In this essay, we study the history of Dirichlet's theorem with an eye towards understanding the methodological pressures that influenced some of the ontological shifts that occurred in nineteenth century mathematics. In particular, we use the history to understand some of the reasons that functions are treated as ordinary objects in contemporary mathematics, as well as some of the reasons one might want to resist such treatment.

§1. Introduction. The philosophy of mathematics has long been concerned with the nature of mathematical objects, and the proper methods for acquiring mathematical knowledge. But as of late, some philosophers of mathematics have begun to raise questions of a broader epistemological character: What does it mean to properly *understand* a piece of mathematics? In what sense can a proof be said to *explain* a mathematical fact? In what senses can one proof be viewed as better than another one that establishes the same theorem? What makes a concept fruitful, and what makes one definition more natural than another? Why are certain historical developments viewed as important advances?

Questions like these are sometimes classified as pertaining to the *methodology* of mathematics, in contrast to more traditional ontological concerns. But methodology and ontology cannot be so cleanly separated. Certainly part of the justification for our ontological commitments stems from the positive effects those commitments have on the practice, and, conversely, "internal" methodological shifts are influenced by a broader conception as to what is permissible.

One of the hallmarks of the nineteenth century transition to modern mathematics was the adoption of implicit or explicit set-theoretic language and methods. For Gauss (1801), the number-theoretic relation of congruence modulo m was a relation that was similar to equality, and addition and multiplication modulo m were operations on integers that respect that relation. Today, however, we can form the quotient structure of integers modulo m, which consists of classes of integers that are equivalent modulo m. Addition and multiplication

Received: November 30, 2014.

This essay draws on the second author's Carnegie Mellon MS thesis Morris (2011). We are grateful to Michael Detlefsen and the participants in his *Ideals of Proof* workshop, which provided helpful feedback on portions of this material in July, 2011. Avigad's work has been partially supported by National Science Foundation grant DMS-1068829 and Air Force Office of Scientific Research grant FA9550-12-1-0370.

doi:10.1017/S1755020315000398

then lift to operations on these classes. This amounts to *reifying* the property of being equivalent to an integer a modulo m to an object, $[a]$, the equivalence class of a. Similarly, to restore the property of unique factorization to the algebraic integers in a cyclotomic field, Kummer (1846) introduced properties $P(\alpha)$ that were meant to be interpreted as the assertion that α is divisible by a certain "ideal divisor." Dedekind (Dirichlet, 1863) later reified the property P to the class of elements α that satisfy it, thereby giving rise to the modern notion of an ideal in a ring of integers. Other nineteenth century examples include the construction of quotient groups, or the lifting of Gauss' operation of "composition" of binary quadratic forms to equivalence classes of such forms.

What these instances have in common is that they involve treating certain higher-order entities—classes of integers, classes of algebraic integers, classes of quadratic forms, or classes of elements in a group or a ring—as objects in their own right. By this we mean that, in particular, one can quantify over them, sum over them, and define operations on them. Moreover, one can consider algebraic structures whose elements are such classes, much as one can consider algebraic structures whose elements are integers or real or complex numbers.

Much of what can be said about the treatment of classes as objects in the nineteenth century applies to the treatment of functions as objects as well. In 1837, Dirichlet proved that there are infinitely many prime numbers in any arithmetic progression in which the terms do not all share a common factor. Our goal here is to study the role that certain types of functions, called *Dirichlet characters*, play in contemporary presentations of Dirichlet's proof, and the historical process that has led to our contemporary understanding.

In Section 2, we present a framework for assessing the ontological commitments of a body of mathematics, one which is informed by, and can inform, the history of mathematics. In Section 3, we provide an overview of Dirichlet's proof, and in Section 4, we clarify the senses in which contemporary presentations treat characters as ordinary mathematical objects. Despite the name, the notion of a Dirichlet character is not present in Dirichlet's original presentation. In Sections 5 and 6, we describe the history of presentations of Dirichlet's theorem, which shows a fitful and gradual transition to modern terminology and usage.

Our presentation draws on a detailed historical study that we have carried out in another work, Avigad & Morris (2014), which we will refer to as "Concept" in the presentation below. For a longer version of this paper, which expands on the ontological considerations and relates them to similar concerns in Frege's work, see Avigad & Morris (unpublished).

§2. From methodology to ontology. It is instructive to consider those historical situations in which the mathematical community faced possibilities for methodological or ontological expansion and reacted accordingly. For example, it is helpful to consider the ancient Greek idealizations of number and magnitude, and the theory of proportion; the gradual acceptance of negative numbers, and then complex numbers, in the Western tradition; the use of algebraic methods in geometry, infinitesimals in the calculus, points at infinity in projective geometry; the development of the function concept from Euler to modern times; the gradual set-theoretic treatment of algebraic objects like cosets, ideals, equivalence classes in the nineteenth century; and so on. By studying the historical concerns regarding these expansions as well as the pressures that led to their ultimate acceptance, we can hope to better understand the factors that influence such developments.

At junctures like these, historical developments tend to follow a common pattern. First, expansions are met with resistance, or at least, extreme caution. Sometimes, the expansions

can be explained in terms of the more conservative practice; for example, complex numbers can be interpreted as ordered pairs, algebraic solutions to geometric problems can be reinterpreted geometrically, and equations can be rewritten to avoid consideration of negative quantities. In other cases, the expansions are not generally conservative, but, at least, can be explained away in particular instances; for example, arguments involving infinitesimals can sometimes be interpreted in terms of "ultimate ratios" in a geometric diagram, and operations on abstract objects can sometimes be understood as operations on explicit representations. This makes it possible to adopt the expansions, tentatively, as convenient shorthand for more tedious but conservative arguments. Over time, the rules and norms that govern the expansions are clarified, and the expansions themselves prove to be convenient, or even indispensable, while they do not cause serious problems. Over time, the mathematical community grows used to them, to the point where they become part of the usual business of mathematics.

Whiggish narratives tend to dismiss such historical hand-wringing and shilly-shallying as short-sighted conservativism that stands in the way of mathematical progress. We, however, prefer to view it as a rational response to the proposed expansions, whereby the benefits are carefully weighed against the concerns. In hindsight, we tend to make too little of the pitfalls associated with an ontological or methodological expansion. To start with, there are concerns about the *consistency* and *coherence* of the new methods, that is, worries as to whether the changes will lead to mistakes, false results, or utter nonsense, perhaps when employed in situations that have not even been imagined. Kenneth Manders has also emphasized the importance of maintaining *control* of our mathematical practices (Manders, 2008). Mathematics requires us to be able to come to agreement as to whether a proof is correct, or whether a given inference is valid or not. If new objects come with rules of use that are not fully specified, or vague, or unclear, the practice is in danger of breaking down. In a sense, this concern comes prior to concerns of consistency: if it is not clear what properties abstract magnitudes, negative numbers, complex numbers, infinitesimals, sets, and "arbitrary" functions have, it doesn't even make sense to ask whether using them correctly will lead to contradictions.[1]

And then there are further concerns as to whether the new methods are *meaningful* and *appropriate* to mathematics. Even if a body of methods is consistent and clearly specified, it may still fail to provide us with the results we are after. If we expect an existence proof to yield certain kinds of information about the object that is asserted to exist, methods that fail to provide that sort of information do not constitute mathematics—or, at least, not the kind of mathematics we should be doing. If you expect a mathematical theory to make scientific predictions that we can act on rationally, it is a serious concern as to whether the new methods can deliver.

In short, the concerns are not easily set aside. What, then, are the factors that might sway a decision in favor of an expansion? Mathematicians tend to wax poetic in their praise of conceptual advances, highlighting the power of new methods, the elegance and naturality of the resulting theory, and the insight and depth of the associated ideas. Part of our goal here is to deromanticize these virtues and gain clarity as to what might be achieved. In many instances, the virtues in question have a lot to do with efficiency and economy of

[1] Mathematics, however, often gets by surprisingly well with concepts that are problematic, incompletely specified, and not fully understood, something which has been emphasized by Wilson (1994) and Urquhart (2008).

thought:[2] we tend to value methods that make it possible to solve problems that were previously unsolvable, or simplify proofs and calculations that were previously tedious, complex, and error-prone. Below we will consider specific ways in which ontological and methodological expansions help us to manage complex tasks by suppressing irrelevant detail, making key features of a problem salient, and keeping key information ready-to-hand. We will also try to understand the way they make it possible to generalize and extend results, and facilitate the transfer of ideas to other domains.

To summarize our high-level historical model: when mathematics is faced with methodological expansion, benefits such as simplicity, generality, and efficiency are invariably weighed against concerns as to the consistency, cogency, and appropriateness of the new methods. Sufficient benefit encourages us to entertain the changes cautiously, while trying to minimize the dangers involved. Cogency is obtained by working out the norms and conventions that govern the new methods. Consistency may not be guaranteed, but our experiences over time can bolster our faith that the new methods do not cause problems. In this regard, initial checks that the new methods are partially conservative over the old ones help to preserve mathematical meaning, and reassure us that even if the new methods turn out to be problematic, one will be able to restrict their scope in such a way that preserves their utility.[3] Our goal here is to consider the history of Dirichlet's theorem in these terms.

§3. An overview of Dirichlet's theorem. Two integers, m and k, are said to be *relatively prime*, or *coprime*, if they have no common factor. In 1837, Dirichlet proved the following:

THEOREM 3.1. *If m and k are relatively prime, the arithmetic progression $m, m+k, m+2k, \ldots$ contains infinitely many primes.*

In other words, if m and k are relatively prime, there are infinitely many primes congruent to m modulo k.

In 1798, Legendre had assumed this, without justification, in a purported proof of the law of quadratic reciprocity. Gauss pointed out this gap, and presented two proofs of quadratic reciprocity in his *Disquisitiones Arithmeticae* of 1801, which do not rely on that fact. He ultimately published six proofs of quadratic reciprocity, and left two more in his *Nachlass*, but he never proved the theorem on primes in an arithmetic progression. Dirichlet's proof is notable not only for settling a longstanding open problem, but also for its sophisticated use of analytic methods to prove a number-theoretic statement.

3.1. Euler's proof that there are infinitely many primes. As Dirichlet himself made clear, the conceptual starting point for his proof lies in the work of Euler. In the *Elements*, Euclid proved that there are infinitely many primes, but his proof does not provide much information about how they are distributed. Euler, in his *Introductio in Analysin Infinitorum* (1748), proved the following:

THEOREM 3.2. *The series $\sum_q \frac{1}{q}$ diverges, where the sum is over all primes q.*

[2] The phrase is borrowed from Ernst Mach's *The Science of Mechanics* (1960); we are grateful to Michael Detlefsen for bringing this to our attention.

[3] Wittgenstein's discussion of contradiction is interesting in this regard; see (Wittgenstein, 1989, Lectures XI–XII).

This implies that there are infinitely many primes, but also says something more about their density. For example, since we know that the series $\sum_n \frac{1}{n^2}$ is convergent, it tells us that, in a sense, there are "more" primes than there are squares.

Euler's proof of Theorem 3.2 centers around his famous zeta function,

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots,$$

defined for a real variable s. (The zeta function was later extended by Riemann to the entire complex plane via analytic continuation.) It is not hard to show that the series $\zeta(s)$ converges whenever $s > 1$. In that case, the infinite sum can also be expressed as an infinite product:

$$\sum_{n=1}^{\infty} n^{-s} = \prod_q \left(1 - \frac{1}{q^s}\right)^{-1}, \tag{1}$$

where the product is over all primes q. This is known as the *Euler product formula*. Roughly, this holds because we can write each term of the product as the sum of a geometric series,

$$\left(1 - \frac{1}{q^s}\right)^{-1} = 1 + q^{-s} + q^{-2s} + \cdots$$

and then expand the product into a sum. The unique factorization theorem tells us that every integer $n > 1$ can be written uniquely as a product $q_1^{i_1} \cdot q_2^{i_2} \cdots q_k^{i_k}$. This means that the term $n^{-s} = q_1^{-i_1 s} \cdot q_2^{-i_2 s} \cdots q_k^{-i_k s}$ will occur exactly once in the expansion, corresponding to the choice of the i_jth element of the sum for each q_j, and the choice of 1 in every other sum. Since we are dealing with infinite sums and products, the Euler product formula implicitly makes a statement about limits, and some care is necessary to make the argument precise; but this is not hard to do.

If we take the logarithm of each side of the product formula and appeal to properties of the logarithm function, we obtain

$$\log \sum_{n=1}^{\infty} n^{-s} = \sum_q -\log\left(1 - \frac{1}{q^s}\right).$$

Using the Taylor series expansion

$$\log(1 - x) = -x - x^2/2 - x^3/3 - \cdots$$

and changing the order of summations yields

$$\log \sum_{n=1}^{\infty} n^{-s} = \sum_q \frac{1}{q^s} + \sum_{n=2}^{\infty} \frac{1}{n} \sum_q \frac{1}{q^{ns}}.$$

Remember that we want to show that $\sum_q \frac{1}{q}$ diverges. Notice that the first term on the right-hand side of the above equation is $\sum_q \frac{1}{q^s}$. Thus we should consider what happens as s tends to 1 from above. One can show that the second term on the right-hand side is bounded by a constant that is independent of s, a fact that can be expressed using "big O" notation as follows:

$$\log \sum_{n=1}^{\infty} \frac{1}{n^s} = \sum_q \frac{1}{q^s} + O(1). \tag{2}$$

As s approaches 1 from above, the left-hand side clearly tends to infinity. Thus, the right-hand side, $\sum_q \frac{1}{q^s}$, must also tend to infinity, which implies that $\sum_q \frac{1}{q}$ diverges.

3.2. Dirichlet's approach. To make the ideas more perspicuous, Dirichlet first considered Theorem 3.1 in the special case where the common difference is a prime number p. Any prime q other than p leaves a remainder of $1, \ldots, p-1$ when divided by p. Splitting up the sum in (2) we then have

$$\log \sum_{n=1}^{\infty} \frac{1}{n^s} = \sum_{q \equiv 1 \bmod p} \frac{1}{q^s} + \sum_{q \equiv 2 \bmod p} \frac{1}{q^s} + \cdots + \sum_{q \equiv p-1 \bmod p} \frac{1}{q^s} + O(1). \qquad (3)$$

This shows that (2) is too crude to prove Theorem 3.1: to show that there are infinitely many primes congruent to m modulo p, we need to show that the mth term on the right-hand side tends to infinity, not just the sum of all such terms. More work is therefore needed to tease apart the contribution of the primes modulo m, for each nonzero residue m modulo p.

Dirichlet sketched his proof in a three-page note announcing the result (Dirichlet, 1837a), before spelling out the details in a later publication (Dirichlet, 1837b). The method relies on a trick that seems to come out of nowhere. We describe the trick here, and in the Appendix we offer an explanation as to how Dirichlet may have come upon this approach.

It is a fact from number theory that for any prime number p, there is a number g, such that the powers $g^0, g^1, g^2, \ldots, g^{p-2}$ modulo p are exactly the nonzero residues $1, 2, 3, \ldots, p-1$ modulo p in some order. Such an element g is called a *primitive root modulo* p. For example, when $p = 11$, we can choose $g = 2$. In that case, the powers of g modulo 11 are

$$1, 2, 4, 8, 5, 10, 9, 7, 3, 6,$$

which are just the numbers from 1 to 10 listed in a different order. Notice that the next element on the list would be 1 again, and the list cycles. In general, if g is a primitive root modulo p, then g^{p-1} is equal to 1 modulo p.

The statement that g is a primitive root modulo p means that for each nonzero residue m modulo p, there is an exponent γ between 0 and $p-2$, with the property that g^γ is equal to m modulo p. We will denote this exponent γ_m and call it the *index* of m modulo p with respect to g, as Dirichlet did. For example, consulting the list above, we see that the index of 10 is 5, because 2^5 is equal to 10 modulo 11. The function $n \mapsto \gamma_n$ behaves like a logarithm, in the sense that if m and n are nonzero residues modulo p, then γ_{mn} is equal to $\gamma_m + \gamma_n$ modulo $p-1$. This is because we have

$$g^{\gamma_m + \gamma_n} = g^{\gamma_m} g^{\gamma_n} = mn \bmod p,$$

and so $\gamma_m + \gamma_n$ modulo $p-1$ is the exponent corresponding to mn.

We now turn our attention from integer roots modulo a prime to the notion of a complex root of unity. In general, if n is any integer, the equation $x^n = 1$ will have n distinct roots in the complex numbers. Moreover, we can choose such a root, ω, that is primitive in the sense that $\omega^0, \omega^1, \omega^2, \ldots, \omega^{n-1}$ are all such roots; taking $\omega = e^{2\pi i/n}$ will do.

Notice that we are now using the phrase "primitive root" in two distinct, but related, senses: to refer to primitive roots modulo a prime, and to refer to primitive roots of unity. For future reference, notice also that the expression $x^n - 1$ factors as $(x-1)(x^{n-1} + \cdots + x^2 + x + 1)$. So, for any complex number x, if x is a solution to $x^n = 1$ other than 1, we have $x^{n-1} + \cdots + x^2 + x + 1 = 0$.

Returning to Dirichlet's theorem, let p be any prime, fix a primitive root g modulo p, and let ω be any $(p-1)$st root of 1, primitive or not. Consider the function $\chi(n)$ which

maps any nonzero residue n to the value ω^{γ_n}. The function χ is *multiplicative*, which is to say, $\chi(mn) = \chi(m)\chi(n)$ for any two nonzero residues m and n. This holds because

$$\chi(mn) = \omega^{\gamma_{mn}} = \omega^{\gamma_m + \gamma_n} = \omega^{\gamma_m}\omega^{\gamma_n} = \chi(m)\chi(n).$$

In the next section, we will see that the functions χ are exactly the *characters* on the group of nonzero residues modulo p. Here, following Dirichlet, we will avoid writing $\chi(n)$ and stick with the notation ω^{γ_n}.

A crucial ingredient in Dirichlet's proof is the observation that the Euler product formula can be generalized. What makes Euler's argument work is the fact that $(1/m^s) \cdot (1/n^s) = 1/(mn)^s$, that is, the fact that the function which maps n to $1/n^s$ is multiplicative. The same argument goes through if we replace the quantity $1/n^s$ by the function

$$\psi(n) = \begin{cases} \omega^{\gamma_n}/n^s & \text{if } n \text{ is not divisible by } p \\ 0 & \text{otherwise.} \end{cases}$$

Thus, generalizing (1), we obtain

$$\sum_{p \nmid n} \frac{\omega^{\gamma_n}}{n^s} = \prod_{p \neq q} \left(1 - \frac{\omega^{\gamma_q}}{q^s}\right)^{-1}.$$

The sum on the left-hand side ranges over numbers n that are not divisible by p, and the product on the right ranges over prime numbers q other than p. Euler's calculation then shows that we have

$$\log \sum_n \frac{\omega^{\gamma_n}}{n^s} = \sum_q \frac{\omega^{\gamma_q}}{q^s} + O(1),$$

in place of (2). Here, the first sum ranges over the same values of n, and the second sum ranges over the same values of q as before. *Now* decompose the sum on the right in terms of the remainder that q leaves when divided by p, and notice that, by definition, γ_q only depends on this remainder. In other words, we have

$$\log \sum_n \frac{\omega^{\gamma_n}}{n^s} = \left(\sum_{q \equiv 1 \bmod p} \frac{1}{q^s}\right)\omega^{\gamma_1} + \left(\sum_{q \equiv 2 \bmod p} \frac{1}{q^s}\right)\omega^{\gamma_2} + \cdots + \left(\sum_{q \equiv p-1 \bmod p} \frac{1}{q^s}\right)\omega^{\gamma_{p-1}} + O(1). \quad (4)$$

The next step involves the trick we alluded to above. Remember, to show that there are infinitely many primes congruent to m modulo p, we want to show that the coefficient of the mth term in the preceding equation, $\sum_{q \equiv m \bmod p} \frac{1}{q^s}$, approaches infinity as s approaches 1. If we let ω be a primitive $(p-1)$st root of 1, then all the roots are given by $\omega^0, \omega^1, \omega^2, \ldots, \omega^{p-2}$. The idea is to plug in all these roots into the preceding equation, and use that to solve for the mth coefficient.

Replacing ω by ω^i in the last equation yields

$$\log \sum_n \frac{\omega^{i\gamma_n}}{n^s} = \left(\sum_{q \equiv 1 \bmod p} \frac{1}{q^s}\right)\omega^{i\gamma_1} + \left(\sum_{q \equiv 2 \bmod p} \frac{1}{q^s}\right)\omega^{i\gamma_2} + \cdots + \left(\sum_{q \equiv p-1 \bmod p} \frac{1}{q^s}\right)\omega^{i\gamma_{p-1}} + O(1).$$

This yields $p-1$ many equations, as i ranges from 0 to $p-2$. To solve for the mth coefficient, for each i, multiply the ith equation by $\omega^{-i\gamma_m}$, and add them.

This is where the magic occurs. If we write L_i for the expression $\sum_{n=1}^{\infty} \frac{\omega^{i\gamma_n}}{n^s}$ that occurs on the left, then the left-hand side of the sum can be written as

$$\log L_0 + \log L_1 \cdot \omega^{-\gamma_m} + \log L_2 \cdot \omega^{-2\gamma_m} + \cdots + \log L_{p-2} \cdot \omega^{-(p-2)\gamma_m}.$$

On the right-hand side, the mth term is exactly

$$(p-1) \cdot \left(\sum_{q \equiv m \bmod p} \frac{1}{q^s} \right),$$

because $\omega^{i\gamma_m} \cdot \omega^{-i\gamma_m} = 1$ for each i, and we are simply summing the same value, $\sum_{q \equiv m \bmod p} 1/q^s$, $p-1$ times. When j is different from m, however, the jth term will be

$$(\omega^{0(\gamma_j - \gamma_m)} + \omega^{1(\gamma_j - \gamma_m)} + \cdots + \omega^{(p-2)\cdot(\gamma_j - \gamma_m)}) \cdot \left(\sum_{q \equiv j \bmod p} \frac{1}{q^s} \right).$$

If we write $\eta = \omega^{\gamma_j - \gamma_m}$, then the coefficient in the last expression is

$$1 + \eta + \eta^2 + \cdots + \eta^{p-2}.$$

But since ω is a $(p-1)$st root of 1, so is η, and since $\gamma_j \neq \gamma_m$, η is not equal to 1. By the observation above, this sum is equal to 0. In other words, all the other terms magically disappear.

Thus we have shown that

$$\log L_0 + \omega^{-\gamma_m} \log L_1 + \omega^{-2\gamma_m} \log L_2 + \cdots + \omega^{-(p-2)\gamma_m} \log L_{p-2} = (p-1) \cdot \sum_{q \equiv m \bmod p} \frac{1}{q^s} + O(1). \quad (5)$$

Solving for $\sum_{q \equiv m \bmod p} 1/q^s$ yields

$$\sum_{q \equiv m \bmod p} \frac{1}{q^s} = \frac{1}{p-1} \Big(\log L_0 + \omega^{-\gamma_m} \log L_1 + \omega^{-2\gamma_m} \log L_2 + \cdots + \omega^{-(p-2)\gamma_m} \log L_{p-2} \Big) + O(1). \quad (6)$$

As a result, we have managed to "extricate" the expression $\sum_{q \equiv m \bmod p} 1/q^s$ from (3). The goal is now to show that this expression approaches infinity as s approaches 1. We now come to the analytic part of Dirichlet's proof: he showed that as s approaches 1, L_0 approaches infinity, but each of the other L_i's approaches a nonzero limit as s approaches 1. This implies that the right-hand side approaches infinity as s approaches 1. Thus the left-hand side approaches infinity as well, which is only possible if there are infinitely many primes congruent to m modulo p.

The presentation here follows Dirichlet's short 1837 presentation fairly closely, though Dirichlet is more terse. As Dirichlet pointed out in that note, the argument can be pushed through for an arbitrary modulus k. But, as we will see in Section 5, the details become unwieldy, and subsequent authors found more convenient ways to express the ideas. In the next section, we explain how the argument above can be described in terms of group characters, and then generalized to the case of an arbitrary modulus.

3.3. Group characters. Let G be a finite abelian group. In contemporary terms, a *character on* G is a function χ from G to the set of nonzero complex numbers with the property that, for every $g_1, g_2 \in G$, $\chi(g_1 g_2) = \chi(g_1)\chi(g_2)$. If g is an element of any finite abelian group, then there is an integer $n > 0$ such that g^n is equal to the identity element of G. This implies that $\chi(g)^n = \chi(g^n) = \chi(1) = 1$. This means that for every g, $\chi(g)$ is a complex root of 1. The notion of "character" introduced in the last section corresponds to the special case where G is the group of nonzero residues modulo p, with the operation of multiplication.

The point is that the key properties of the expressions ω^{γ_n} that came into play in the last section hold more generally of the set of characters on any finite abelian group. In particular, for any such group G, one can show that there are exactly $|G|$ many distinct characters on G, where $|G|$ denotes the number of elements of G. In the case where G is the group of nonzero residues modulo p, $|G| = p - 1$, so the characters correspond to the $p - 1$ choices of ω in the previous section. More generally, for any $k \geq 1$, the set of residues m modulo k that have no common factor with k form a group under multiplication. The cardinality of this group is commonly denoted $\varphi(k)$, and φ is known as the Euler phi function. Thus, for every k, there are $\varphi(k)$ many characters on the group of residues modulo k.

In fact, the set of characters itself has the structure of a group $\widehat{G}$, where the identity is the character χ_1 that always returns 1, and the product of two characters is given pointwise, $(\chi \cdot \chi')(g) = \chi(g)\chi'(g)$ for every g. The following theorem expresses two important properties, known as the "orthogonality relations" for group characters.

THEOREM 3.3. *Let G be a finite abelian group. Then for any character χ in $\widehat{G}$, we have*

$$\sum_{g \in G} \chi(g) = \begin{cases} |G| & \text{if } \chi = \chi_0 \\ 0 & \text{if } \chi \neq \chi_0, \end{cases}$$

and for any element g of G, we have

$$\sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} |G| & \text{if } g = 1_G \\ 0 & \text{if } g \neq 1_G. \end{cases}$$

The remarkable fact is that it is no harder to prove these facts in the general case than in the specific case where G is a group of residues modulo p. For example, the second equation clearly holds when g is the identity of G, since, in this case, each term of the sum is equal to 1. Otherwise, choose a character ψ such that $\psi(g) \neq 1$ and note

$$\psi(g) \sum_{\chi \in \widehat{G}} \chi(g) = \sum_{\chi \in \widehat{G}} \psi(g)\chi(g) = \sum_{\chi \in \widehat{G}} \chi(g),$$

since multiplying each character χ in $\widehat{G}$ by ψ simply permutes the elements of $\widehat{G}$. Subtracting the right side of the equation from the left, we see that $(\psi(g) - 1) \cdot \sum_{\chi \in \widehat{G}} \chi(g) = 0$, and since $\psi(g)$ is not equal to 1, we have that $\sum_{\chi \in \widehat{G}} \chi(g) = 0$. The first equation can be established in a similar way.

The second orthogonality relation gives rise to the "cancellation trick" used in the last section, where we multiplied each identity by $\omega^{-i\gamma_m}$ and added them, to isolate a particular coefficient. The general phenomenon can be expressed as follows:

COROLLARY 3.4. *For any $g, h \in G$ we have the following:*

$$\sum_{\chi \in \widehat{G}} \chi(g)\overline{\chi(h)} = \begin{cases} |G| & \text{if } g = h \\ 0 & \text{if } g \neq h. \end{cases}$$

Here $\bar{z}$ denotes the complex conjugate of z, which is in fact equal to $1/z$ when z is a root of unity. The corollary follows from the fact that we have

$$\sum_{\chi \in \widehat{G}} \chi(g)\overline{\chi(h)} = \sum_{\chi \in \widehat{G}} \chi(g)\chi(h)^{-1} = \sum_{\chi \in \widehat{G}} \chi(gh^{-1}) = \begin{cases} |G| & \text{if } g = h \\ 0 & \text{if } g \neq h. \end{cases}$$

Notice that the abstract algebraic formulation simplifies matters by eliminating clutter. For example, the presentation in the last section depended on choices of a primitive element g modulo p, and a primitive $(p-1)$st root of unity ω. Although these played a role in the computations, any choice of g and ω works just as well. The abstract version "factors these out" of the presentation. Recall also that the calculation in the last section required facts such as $\gamma_{mn} = \gamma_m + \gamma_n$. Once again, the abstract version factors this out of the computation; the requisite property of γ subsumed by the more general fact that $\widehat{G}$ is a group, and only the latter fact enters into the proof.

3.4. A modern formulation of Dirichlet's proof. With the notion of a group character in mind, we can now describe Dirichlet's original proof of Theorem 3.1 in modern terms. Let k be an integer greater than or equal to 1. It is a fundamental theorem of number theory that an integer n is relatively prime to k if and only if n has a multiplicative inverse modulo k; in other words, if and only if there is some n' such that $nn' \equiv 1 \bmod k$. This implies that the residues of integers modulo k that are relatively prime to k form a group, denoted $(\mathbb{Z}/k\mathbb{Z})^*$, with multiplication modulo k. As noted above, the cardinality of $(\mathbb{Z}/k\mathbb{Z})^*$, that is, the number of residues relatively prime to k, is denoted $\varphi(k)$.

A character χ on the group of residues modulo k can be viewed as a function defined on all integers by

$$X(n) = \begin{cases} \chi(n \bmod k) & \text{if } n \text{ is relatively prime to } k \\ 0 & \text{otherwise.} \end{cases}$$

Such a function is called a *Dirichlet character modulo k*. Dirichlet characters are *completely multiplicative*, which is to say, $X(1) = 1$ and $X(mn) = X(m)X(n)$ for every m and n in $\mathbb{Z}$. Mathematicians typically use the symbol χ to range over Dirichlet characters, blurring the distinction between such functions and their group-character counterparts. This is harmless, since there is a one-to-one correspondence between the two, and so we will adopt this practice as well.

Recall that in the case where k is a prime number p, Dirichlet considered certain expressions $L_i(s)$, analogues of Euler's zeta function, where i is an integer between 0 and $p-2$. Each such i corresponds to a choice of a character χ modulo p. In the modern formulation, then, we define

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

where χ is such a character. The function $L(s, \chi)$ is called the *Dirichlet L-function*, or *L-series*.

The calculation in Section 3.2 can be generalized to show:

$$\log L(s, \chi) = \sum_{q \nmid k} \frac{\chi(q)}{q^s} + O(1).$$

Now comes the crucial use of Corollary 3.4 to pick out the primes in the relevant residue class. We multiply each side of the above equation by $\overline{\chi(m)}$ and then take the sum of these over all the Dirichlet characters modulo k. (Recall that we can identify each Dirichlet character with the corresponding group character, that is, the corresponding element of $\widehat{(\mathbb{Z}/k\mathbb{Z})^*}$.) Thus we have:

$$\sum_{\chi \in \widehat{(\mathbb{Z}/k\mathbb{Z})^*}} \overline{\chi(m)} \log L(s, \chi) = \sum_{\chi \in \widehat{(\mathbb{Z}/k\mathbb{Z})^*}} \overline{\chi(m)} \sum_{q \nmid k} \frac{\chi(q)}{q^s} + O(1).$$

To simplify this expression, we exchange the summations on the right-hand side, and appeal to Corollary 3.4. Since the cardinality of the group $(\mathbb{Z}/k\mathbb{Z})^*$ is $\varphi(k)$, we obtain

$$\sum_{\chi \in \widehat{(\mathbb{Z}/k\mathbb{Z})^*}} \overline{\chi(m)} \log L(s, \chi) = \varphi(k) \sum_{q \equiv m \pmod{k}} \frac{1}{q^s} + O(1). \tag{7}$$

This is analogous to the equation (2) in Euler's proof, and equation (5) in Section 3.2. Our goal is once again to show that the left-hand side tends to infinity as s approaches 1 from above. This implies that the right-hand side tends to infinity, which, in turn, implies that there are infinitely many primes q that are congruent to m modulo k.

To show that $\sum_{\chi \in \widehat{(\mathbb{Z}/k\mathbb{Z})^*}} \overline{\chi(m)} \log L(s, \chi)$ tends to infinity as s approaches 1, we divide the characters into three classes, as follows:

1. The first class contains only the principal character χ_0, which takes the value of 1 for all arguments that are relatively prime to k, and 0 otherwise.
2. The second class consists of all those characters which take only real values (i.e. 0 or ± 1), other than the principal character.
3. The third class consists of those characters which take at least one complex value.

It is not difficult to show that $L(s, \chi_0)$ has a simple pole at $s = 1$, which implies that the term $\overline{\chi_0}(m) \log L(s, \chi_0)$ approaches infinity as s approaches 1. The real work involves showing that for all the other characters χ, $L(s, \chi)$ has a finite nonzero limit. This implies that the other terms in the sum approach a finite limit, and so the entire sum approaches infinity.

For characters in the third class, that is, the characters that take on at least one complex value, the result is not difficult. For characters in the second class, the result is much harder, and Dirichlet used deep techniques from the theory of quadratic forms to obtain it. In the years that followed, other mathematicians found alternative, and simpler ways of handling this case. But even in modern presentations, this case remains the most substantial and technically involved part of the proof.

§4. Functions as objects. In Section 5 below, we will discuss, in greater detail, the implicit treatment of characters in Dirichlet's original proof, and in Section 6, we will summarize the gradual historical transition to the modern formulation. The general theme will be that, over time, characters came to be treated as objects in their own right. Before surveying the history, however, it will be helpful for us to provide some general background

information on the nineteenth century concept of "function," and begin to spell out what it means to treat functions like characters as "objects."

In "Concept," we discussed a number of nineteenth-century methodological changes that are clustered around the function concept. These include what we termed the "unification" or "generalization" of the function concept, whereby particular instances (including real- and complex-valued functions, number-theoretic functions, sequences, permutations, transformations, automorphisms, and so on) gradually came to be subsumed under a general notion; the "liberalization" of the function concept, whereby mathematicians adopted novel means of defining particular functions, such as Dirichlet's 1827 example of a real-valued function that takes one value on the rationals, and another value on the irrationals; the "extensionalization" of the function concept, whereby functions gradually came to be viewed less as syntactic or algebraic expressions, and more as the abstract entities denoted by such expressions; and the "reification" of the function concept, whereby functions were gradually treated as *bona fide* mathematical objects.

The notion of "reification" is vague. The claim that over the course of the century characters gradually become treated as new sorts of objects supports our contention that the transformation has ontological overtones, but it raises serious questions as to what, exactly, it means to treat certain entities as objects.

To start with, consider the fact that in our presentation of Dirichlet's theorem we identified the concept of a "character," reasoned about the entities falling under this concept, and ascribed various properties to them. This seems to be a bare-minimum requirement to support the claim that a mathematical text sanctions certain entities as objects, namely, that it recognizes them as being entities of a certain *sort*, capable of bearing predicates and being the target of certain operations. It does not matter whether we take this sort as fundamental (for example, as we take the notion of "integer" in most contexts) or as derived from a broader sort (for example, when we view characters as functions of a certain kind). What is important is that the entities belong to a grammatically recognized category, and this category helps to determine the predicates and operations that can be meaningfully ascribed to it. For example, one can talk about one integer being larger than another, but not one character as being larger than another. In sum, our first criterion of objecthood is whether the entities in question have a recognizable role in the grammar of the language.

The fact that we took characters to be "represented" by certain symbolic expression provides another clue, insofar as we generally speak of a representation *of* something or other. For example, we think of expressions like "6" and "2×3" as representing an integer. As Michael Detlefsen has pointed out to us, one common view is that an "object" is what remains invariant under all its representations; in other words, what is left over when one has "squeezed out" all the features that are contingent on particular representations. When it comes to the notion of a function, what is the underlying invariant? There may be lots of ways of describing a particular function, but what makes them representations of the *same* function is surely that they take the same values on any given input. Thus treating function expressions extensionally is a sign that one is reasoning about functions as objects, rather than reasoning about the expressions themselves.[4]

The third hallmark of object-hood that is present in our list is evidenced by the fact that we can *sum* over characters, just as we can sum over natural numbers. Notice that in an expression $\sum_{\chi} \ldots \chi \ldots$, the variable χ is a bound variable that ranges over the entities in question. Similar considerations hold for the universal and existential quantifiers.

[4] Recall Quine's dictum that "there is no entity without identity," for example in Quine (1969).

Viewing the natural numbers as quintessential mathematical objects, a sign that an entity has attained the status of object-hood is that it is possible to quantify over them in theorems and definitions, just as one quantifies over the natural numbers.[5] The consideration admits of degrees: whereas the bare-minimum requirement discussed above may allow us to state theorems about, and define operations on, "arbitrary" entities of the sort, a more full-blown notion of object-hood will give us more latitude in the kinds of quantification and binding that are allowed.

The fourth criterion for object-hood is evidenced by the fact that characters are allowed to appear as *arguments* to the L-functions, for example, in the expression $L(s, \chi)$. To avoid making this consideration depend on the modern notion of a function, let us note that what is essential here is that an expression denoting a recognized mathematical object (in this case, a complex number) is allowed to *depend* on a character, much the way that a real number $(s)_i$ in a sequence depends on the value of the index i, or a value $\varphi(n)$ of the phi function depends on n. What makes this more potent than the mere ability to define operations on characters is that the dependent expressions are treated as objects in their own right. $L(s, \chi)$ is not just an operation on s and χ: fixing χ, the function $s \mapsto L(s, \chi)$ is an object that one can integrate and differentiate, and fixing s, we can sum over the values obtained by varying χ.

It is also notable that the characters can be components in the construction of other mathematical objects and structures. For example, one can form sets and sequences of characters, in much the same way that one forms sets and sequences of numbers, and one can define a group whose elements are characters, in much that same way that one can form a group whose elements are residues modulo some number m.

To summarize, here are some of the various senses in which one might say that characters are treated "as objects" in our presentation of Dirichlet's proof:

1. Characters fall under a recognized grammatic category, which allows us to state things about them and define operations and predicates on them.
2. There is a clear understanding of what it means for two expressions to represent the *same* character, and conventions ensure that the expressions occurring in a proof respect this "sameness."
3. One can quantify and sum over characters; in other words, they can fall under the range of a bound variable.
4. One can define functions which take characters as arguments.
5. One can construct new mathematical entities, like sets and sequences, whose elements are characters. In particular, characters can be elements of an algebraic structure like a group.

We recognize that determining the "ontological commitments" of a practice may not be as clear-cut as Quine's writings suggest. Our goal here is not to explicate what it means to say that a certain manner of discourse is committed to treating some entity as an object. In particular, we do not claim to have given a precise sense to the question as to whether a particular mathematical proof is committed to functions as objects. We do claim, however, to have identified various important senses in which contemporary proofs of Dirichlet's theorem treat functions as ordinary mathematical objects, whereas Dirichlet's original proof did not.

[5] This echoes another Quine dictum, "to be is to be the value of a bound variable" (Quine, 1948, p. 15).

It may be helpful to compare the way we treat functions today to the way we treat natural numbers today. For example, the expressions "$2 + 2$" and "4" both denote integers, but we think of the number as the object denoted, rather than the expression. Thus we can send numbers as arguments to functions, and when we write $f(2 + 2)$ and $f(4)$, it is understood that the function f cannot distinguish the mode of presentation. We can form sets of numbers, like the set of even number or the set of prime numbers, and we can consider algebraic structures on these sets; for example, the ring of integers, or the field of integers modulo 7. We can quantify over numbers in definitions, such as when we say n divides m if there is some k such that $nk = m$, and in theorems, such as when we assert that every integer greater than one has a prime divisor. If S is a finite set of integers and f is a function from the integers to the integers or the reals, we can readily form the sum $\sum_{x \in S} f(x)$.

In contemporary mathematics, nothing goes awry if you replace integers with functions in the examples in the last paragraph. In other words, one can define functionals $F(f)$ that depend only on the extension of f, and not its manner of presentation. We can consider sets of functions, rings of functions, and spaces of functions. We quantify over functions in definitions and theorems, and, if S is a finite set of functions, we think nothing of considering a sum $\sum_{f \in S} F(f)$. In the proof of Dirichlet's theorem, these "higher order" operations are manifest when we consider the group of characters χ, define the Dirichlet L series $L(s, \chi)$, and form the sum $\sum_{\chi} \overline{\chi(m)} \log L(s, \chi)$.

In "Concept," we argued in detail that these very features of the modern treatment of functions were alien to early nineteenth century mathematics, and that the history of presentations of Dirichlet's theorem shows a very gradual evolution, in fits and starts, towards the contemporary manner of thought. We will highlight some of the key features of the historical development in Sections 5 and 6, and, in Section 7, explore what the history tells us about the nature of mathematics.

§5. Dirichlet's treatment of characters. Contemporary mathematicians are often surprised to hear that there is no explicit notion of "character" in Dirichlet's 1837 proof. After all, the expressions $X(n)$ defined in Section 3.4 are known as "Dirichlet characters" precisely because of their implicit use in that proof. But Dirichlet did not introduce notation for the characters or refer to them as such. When we speak of the "characters" in his proof, we are projecting a modern interpretation onto the symbolic expressions that appear there.

Remember how it works in the case where the common difference is a prime, p. Let g be a primitive element modulo p, and for every n coprime to p, let γ_n denote the index of n with respect to g, so that $g^{\gamma_n} \equiv n \bmod p$. Then each character χ corresponds to a $(p-1)$st root of unity ω, with defining equation $\chi(n) = \omega^{\gamma_n}$. In that case, Dirichlet wrote ω^{γ_n} where we would write $\chi(n)$.

We obtain all the characters by picking a primitive $(p-1)$st root of unity, Ω, so that all the $(p-1)$st roots of unity are given by the sequence $\Omega^0, \ldots, \Omega^{p-2}$. This provides a convenient numbering scheme for the characters and L-series: Dirichlet used L_m to denote the L-series based on the character χ that corresponds to Ω_m, where we would write instead $L(s, \chi)$. And where we would form a summation over the set of all characters, Dirichlet instead took a summation over the values $0, \ldots, p-2$. For example, after demonstrating the Euler product formula,

$$\prod \frac{1}{1 - \omega^{\gamma} \frac{1}{q^s}} = \sum \omega^{\gamma} \frac{1}{n^s} = L,$$

Dirichlet wrote:

> The equation just found represents $p-1$ different equations that result if we put for ω its $p-1$ values. It is known that these $p-1$ different values can be written using powers of the same Ω when it is chosen correctly, to wit:
>
> $$\Omega^0,\ \Omega^1,\ \Omega^2,\ \ldots,\ \Omega^{p-2}.$$
>
> According to this notation, we will write the different values L of the series or product as:
>
> $$L_0,\ L_1,\ L_2,\ \ldots,\ L_{p-2}.$$

In the case where the modulus k is not prime, the procedure is more complicated. It is a fundamental theorem of group theory that every finite abelian group can be represented as a product of cyclic groups, but that theorem was first proved by Kronecker (1870). Dirichlet instead used the particular instance of this fact for the group $(\mathbb{Z}/k\mathbb{Z})^*$ of residues modulo k that are relatively prime with k (these are sometimes called the "units" modulo k). The structure of that group was known to Gauss. First, write k as a product of primes,

$$k = 2^\lambda p_1^{\pi_1} p_2^{\pi_2} \cdots p_j^{\pi_j}$$

where each p_i is an odd prime and π_i is greater than or equal to 1. Then the group of units modulo k is isomorphic to the product of the groups of units modulo each term in the factor. If p is an odd prime and π is an integer greater than or equal to 1, then one can more generally find a primitive element c modulo p^π. This means that the residue class of c generates the cyclic group $(\mathbb{Z}/p^\pi\mathbb{Z})^*$, or, equivalently, for every n relatively prime to p there is a γ_n such that $c^{\gamma_n} \equiv n \bmod p^\pi$. Thus we can choose primitive elements $c_1, \ldots, c_j$ corresponding to $p_1^{\pi_1}, p_2^{\pi_2}, \ldots, p_j^{\pi_j}$. If $\lambda \geq 3$, however, there is no primitive element modulo 2^λ. Rather, $(\mathbb{Z}/2^\lambda)^*$ is a product of two cyclic groups, and for every n relatively prime to 2^λ there are an α_n and β_n such that $(-1)^{\alpha_n} 5^{\beta_n} \equiv n \bmod 2^\lambda$. Thus for any n relatively prime to k, we can write

$$n \equiv (-1)^{\alpha_n} 5^{\beta_n} c_1^{\gamma_{1,m}} c_2^{\gamma_{2,m}} \ldots c_j^{\gamma_{j,m}} \bmod k,$$

where each $\gamma_{i,n}$ is the index n relative to $p_i^{\pi_i}$. As above, if we choose appropriate roots of unity $\theta, \varphi, \omega_1, \omega_2, \ldots, \omega_j$, we obtain a character

$$\chi(n) = \theta^{\alpha_n} \varphi^{\beta_n} \omega_1^{\gamma_{1,n}} \omega_2^{\gamma_{2,n}} \cdots \omega_j^{\gamma_{j,n}}.$$

And, once again, every character is obtained in this way. We should note that Dirichlet used the notation $p, p', \ldots$ rather than $p_1, \ldots, p_j$ to denote the sequence of odd primes. Moreover, he used the notation $\alpha, \beta, \gamma, \gamma', \ldots$ to denote the indices, suppressing the dependence on n. Thus, Dirichlet wrote $\theta^\alpha \varphi^\beta \omega^\gamma \omega'^{\gamma'} \ldots$ for the expression we have denoted $\chi(n)$ above, leaving it up to us to keep in mind that $\alpha, \beta, \ldots$ depend on n.

To summarize, in the simple case of a prime modulus p, Dirichlet fixed a primitive element modulo c, and represented each character χ in terms of a $(p-1)$st root of unity, ω. In that case, the value $\chi(n)$ is given by ω^{γ_n}. In the more general case of a composite modulus k, Dirichlet fixed primitive elements modulo the terms of the prime factorization of k, and represented each character χ in terms of a sequence $\theta, \varphi, \pi, \pi'$ of roots of unity. In that case, the value $\chi(n)$ was written $\theta^\alpha \varphi^\beta \omega^\gamma \omega'^{\gamma'} \ldots$, suppressing the information that

the exponents $\alpha, \beta, \gamma, \gamma', \ldots$ depend on n. For example, he described the Euler product formula as follows:

$$\prod \frac{1}{1 - \theta^{\alpha}\varphi^{\beta}\omega^{\gamma}\omega'^{\gamma'} \cdots \frac{1}{q^{s}}} = \sum \theta^{\alpha}\varphi^{\beta}\omega^{\gamma}\omega'^{\gamma'} \cdots \frac{1}{n^{s}} = L, \tag{8}$$

> where the multiplication sign ranges over all primes, with the exclusion of 2, $p, p', \ldots$, and the summation ranges over all the positive integers that are not divisible by any of the primes 2, $p, p', \ldots$. The system of indices $\alpha, \beta, \gamma, \gamma', \ldots$ on the left side corresponds to the number q, and on the right side to the number n. The general equation (8), in which the different roots $\theta, \varphi, \omega, \omega', \ldots$ can be combined with one another arbitrarily, clearly contains K-many particular equations. (Dirichlet, 1837b, p. 17; equation number changed)

Note, again, Dirichlet's characterization of the general equation as "containing" the particular instances. Here, K is what we have called $\varphi(k)$, the cardinality of the group $(\mathbb{Z}/k\mathbb{Z})^*$.

Dirichlet went on to observe that we can choose primitive roots of unity $\Theta, \Phi, \Omega, \Omega', \ldots$ so that all choices of $\theta, \varphi, \omega, \omega', \ldots$ can be expressed as powers of these,

$$\theta = \Theta^{\mathfrak{a}}, \varphi = \Phi^{\mathfrak{b}}, \omega = \Omega^{\mathfrak{c}}, \omega' = \Omega^{\mathfrak{c}'}, \ldots,$$

just as in the simpler case. He wrote that we can thus refer to the L-series in a "convenient" (*bequem*) way, as $L_{\mathfrak{a},\mathfrak{b},\mathfrak{c},\mathfrak{c}',\ldots}$, where $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{c}', \ldots$ are the exponents of the chosen primitive roots. Notice that the representations just described depend on fixed, but arbitrary, choices of the primitive roots of unity, as well as fixed but arbitrary generators of the cyclic groups. Modulo those choices, we have parameters $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{c}', \ldots$ that vary to give us all the characters; and for each choice of $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{c}', \ldots$ we have an explicit expression that tells us the value of the character at n.

For Dirichlet, summing over characters therefore amounted to summing over all possible choices of this representing data. In the special case of where the common difference is a prime, p, Dirichlet ran through calculations similar to those described in Section 3.4 to obtain the following identity:

$$\sum \frac{1}{q^{1+\rho}} + \frac{1}{2}\sum \frac{1}{q^{2+2\rho}} + \frac{1}{3}\sum \frac{1}{q^{3+3\rho}} + \cdots$$
$$= \frac{1}{p-1}(\log L_0 + \Omega^{-\gamma_m} \log L_1 + \Omega^{-2\gamma_m} \log L_2 + \cdots + \Omega^{-(p-1)\gamma_m} \log L_{p-2}).$$

This is exactly equation (6) above, with Ω in place of our ω, and $1 + \rho$ in place of s, and the "$O(1)$" expression left explicit. In the more general case, he arrived at the analogous result:

$$\sum \frac{1}{q^{1+\rho}} + \frac{1}{2}\sum \frac{1}{q^{2+2\rho}} + \frac{1}{3}\sum \frac{1}{q^{3+3\rho}} + \cdots$$
$$= \frac{1}{K}\sum \Theta^{-\alpha_m \mathfrak{a}}\, \Phi^{-\beta_m \mathfrak{b}} \Omega^{-\gamma_m \mathfrak{c}} \Omega^{-\gamma'_m \mathfrak{c}'} \cdots \log L_{\mathfrak{a},\mathfrak{b},\mathfrak{c},\mathfrak{c}',\ldots}.$$

Here the summation on the right-hand side of the equation is over the possible values of $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{c}', \ldots$. This corresponds to equation (7) in Section 3.4.

Finally, recall from the sketch in Section 3.4 that Dirichlet divided the L functions into three classes, depending on whether the corresponding character was trivial (identically

equal to 1), real-valued, or complex-valued. But in Dirichlet's presentation, the categorization was made in terms of the *roots used to describe the character*. Thus the three classes of L functions were characterized as follows:

1. the one in which all the roots contained in the expression are 1
2. those, among the ones that remain, in which all the roots are real (± 1)
3. those in which at least one of the roots is not real

Dirichlet showed that the first approaches infinity as ρ approaches 0, while the others approach finite limits, which establishes the desired conclusion.

Let us summarize the features of Dirichlet's presentation we wish to highlight. First, he did not name or identify the characters, and simply used the corresponding algebraic expressions. The corresponding L functions were then characterized by the data that appeared in the expression, rather than in terms of a functional dependence on the character. In other words, Dirichlet wrote L_m or $L_{a,b,c,c',\ldots}$ where we would write $L(s, \chi)$. As a result, where we would sum an expression over all values of the characters $\sum_\chi \ldots$, he summed over the representing data $\sum_m \ldots$ or $\sum_{a,b,c,c',\ldots} \ldots$. Finally, in preparation for the analytic part of the proof, he sorted the L functions in terms of this data, rather than in terms of the values of the corresponding characters.

In the next section, we will see that, over time, all of these features were gradually eliminated from later expositions.

§6. The transition to the modern treatment of characters. In "Concept," we studied the treatment of characters in subsequent works by Dirichlet (1840, 1841), Dedekind's supplements to the first two editions of (Dirichlet, 1863), work by Kronecker from the 1870's that was eventually published in (Kronecker, 1901), and works by Weber (1882), Hadamard (1896), de la Vallée Poussin (1897), and Landau (1909, 1927). We will not review all the details here, but, rather, summarize the salient features of the history.

6.1. Reification. We have seen that in Dirichlet's original proof, characters are present only in the form of the algebraic expressions ω^{γ_n} in the simple case, and in the form $\theta^{\alpha_n}\varphi^{\beta_n}\omega^{\gamma_n}\omega'^{\gamma'_n}\ldots$ in the case of an arbitrary modulus. In 1841, however, Dirichlet considered expressions

$$\Omega_n = \varphi^{\alpha_n}\varphi'^{\alpha'_n} \times \cdots \times \psi^{\beta_n}\chi^{\gamma_n}\psi'^{\beta'_n}\chi'^{\gamma'_n} \times \cdots \times \theta^{\delta_n}\eta^{\varepsilon_n},$$

analogous to the characters in his 1837 proof. In this case, however, he introduced the explicit notation Ω_n, and isolated four key properties of these values:

1. $\Omega_{nn'} = \Omega_n\Omega_{n'}$ for every n and n'.
2. $\Omega_{n'} = \Omega_n$ whenever $n' \equiv n \pmod{k}$.
3. $\sum \Omega_l = 0$ or $\sum \Omega_l = \frac{1}{4}\psi(k)$ depending on whether there is at least one root among the roots in Ω_l that is different to 1, or whether they are all equal.
4. $S\Omega_n = \frac{1}{4}\psi(k)$ or $S\Omega_n = 0$ depending on whether $n \equiv 1 \pmod{k}$ or $n \not\equiv 1 \pmod{k}$, where the sign "S" indicates a sum over all combinations of the roots that can occur in Ω.

In modern terms, the first clause asserts that the function $n \mapsto \Omega_n$ is a multiplicative function from the integers to the complex numbers, and the second asserts that the value Ω_n only depends on the value of n modulo p. If you add the constraints that Ω_n is nonzero when n is relatively prime to k and zero otherwise, this is exactly the algebraic definition

of character we presented in Section 3.3. The third and fourth properties correspond to the two orthogonality relations we presented in Section 3.3. The article provided only a short sketch of a generalization of his 1837 proof, but it is notable that there Dirichlet went out of his way to flag these expressions as playing a key role, and to abstract away the general properties that are common to both proofs.

In 1863, Dedekind gave an exposition of Dirichlet's proofs in one of the appendices, or "supplements," to the first edition of his presentation of Dirichlet's lectures on number theory Dirichlet (1863). When presenting the generalization of the Euler product formula, he went out of his way to point out that the function

$$\psi(n) = \frac{\theta^{\alpha}\eta^{\beta}\omega^{\gamma}\omega'^{\gamma'}\cdots}{n^{s}}$$

is multiplicative, and that this is what makes the generalization hold. In a later 1871 edition of the work, he added a footnote, in which he singled out the numerator of this expression, and introduced the notation $\chi(n)$:

> The numerator [of $\psi(n)$] $\chi(n) = \theta^{\alpha}\eta^{\beta}\omega^{\gamma}\omega'^{\gamma'}\cdots$ has the characteristic property $\chi(n)\chi(n') = \chi(nn')\ldots$ (Dirichlet, 1863, §133, footnote).

It is notable that he went out of his way to add this footnote, calling attention to the importance of these expressions.[6]

In 1879, in the third edition of the lectures, Dedekind introduced the notion of a character in an entirely different context: his theory of ideals in an algebraic number field. Rather than considering characters on the multiplicative group of residues modulo an integer, he considered characters defined on another finite abelian group, namely, on the class group in an algebraic number field:

> ...the function $\chi(\mathfrak{a})$ also possesses the property that it takes the same value on all ideals $\mathfrak{a}$ belonging to the same class A; this value is therefore appropriately denoted by $\chi(A)$ and is clearly always an hth root of unity. Such functions χ, which in an extended sense can be termed *characters*, always exist; and indeed it follows easily from the theorems mentioned at the conclusion of §149 that the class number h is also the number of all distinct characters $\chi_1, \chi_2, \ldots, \chi_h$ and that every class A is completely characterized, i.e. is distinguished from all other classes, by the h values $\chi_1(A), \chi_2(A), \ldots, \chi_h(A)$.[7]

As we emphasize in "Concept," this was not only the first use of the term "character" in its modern sense, but also, as far as we know, the earliest instance of the use of the term "function" for something defined on a domain other than the integers, real numbers, or complex numbers. (Another broad use of the term occurs in Frege's *Begriffsschrift*, which was published in the same year.) Within three years, in an 1882 publication, Weber gave the general definition of a character of an abelian group and provided a thorough analysis of their properties.

---

[6] In "Concept," we mistakenly asserted that Dedekind did not alter the text of this supplement in later editions. He made very few such changes, however, making this particular addition especially interesting.

[7] The quotation appears in §178 in the 1879 edition of the *Vorlesungen* Dirichlet (1863), and in §184 of the 1894 edition, which is reproduced in Dedekind's *Werke* Dedekind (1968). The translation above is by (Hawkins, 1971, p. 149).

Thus, over time, the symbolic expressions appearing in Dirichlet's proof were named and flagged as entities worthy of attention. Their properties were stated abstractly, and developed in a manner that were independent of the original formulation. This, in turn, made it possible to apply the notion in other settings. As we have argued in Section 4, this provides at least a minimal sense in which characters can be viewed as objects, namely, as entities which can bear properties and be a target of assertions.

6.2. Functional dependence and summation. In Section 4, we also flagged it as notable that, in the modern view, functions can depend on characters, and we can form the sum of an expression with a variable ranging over the characters. Let us consider the way these features of the treatment of characters play out in the various presentations of Dirichlet's theorem.

We have noted that one benefit of identifying the characters as such is that it facilitates extracting the central properties that play a role in the proof, such as the identity

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

in Theorem 3.3, and the consequence expressed by Corollary 3.4 that for every g and h in an abelian group G,

$$\sum_{\chi \in \widehat{G}} \chi(g)\overline{\chi(h)} = \begin{cases} |G| & \text{if } g = h \\ 0 & \text{if } g \neq h. \end{cases}$$

In the case where G is the group of nonzero residues modulo p, Dirichlet expressed the latter by saying that we have

$$1 + \Omega^{h\gamma - \gamma_m} + \Omega^{2(h\gamma - \gamma_m)} + \cdots + \Omega^{(p-2)(h\gamma - \gamma_m)} = 0,$$

except when $h\gamma - \gamma_m \equiv 0 \bmod p - 1$, in which case the sum is equal to $p - 1$. In the case of an arbitrary modulus, Dirichlet did not even state the conclusion as a separate result. Rather, it is implicitly contained in an argument in which he considered the sum $\frac{1}{h} \sum W \frac{1}{q^{h+h\rho}}$,

> ... where the symbol $\sum$ ranges over all primes q and W denotes the product of the sums taken over $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{c}', \ldots$ or respectively over
>
> $$\sum \Theta^{(h\alpha - \alpha_m)\mathfrak{a}}, \sum \Phi^{(h\beta - \beta_m)\mathfrak{b}}, \sum \Omega^{(h\gamma - \gamma_m)\mathfrak{c}}, \sum \Omega'^{(h\gamma' - \gamma'_m)\mathfrak{c}'}, \ldots.$$
>
> (Dirichlet, 1837b, p. 340)

This makes it harder to appreciate the nature of the cancellation trick. Moreover, although values $\Theta, \Phi, \Omega, \Omega', \ldots$ can be used to define the individual characters, these tuples and the corresponding representation play no role in the subsequent proof, which depends only on the orthogonality relations and the multiplicative nature of the characters. It seems reasonable, then, to seek a manner of expression that abstracts away the details of the representation. We saw that in his 1841 paper on arithmetic progressions in the quadratic integers, Dirichlet briefly used the expression $S\Omega_n$ to denote the result of summing the values of Ω_n over all possible combinations of roots that occur in Ω. Kronecker maintained the dependence of the characters on the defining tuples of data, but found a much more elegant notation for expressing the dependence. He denoted the character corresponding to the tuple of parameters (k) by $\Omega^{(k)}$, and in the case of a modulus m, he expressed the

second orthogonality relation by writing

$$\sum_{(k)} \Omega^{(k)}(r_0) = \varphi(m),$$

when r_0 is congruent to 1 modulo m, and

$$\sum_{(k)} \Omega^{(k)}(r) = 0$$

otherwise. In his 1883 paper on general characters, Weber adopted a curious means of abstracting the representation of the characters: he simply assigned arbitrary indices to the characters, listing them as $\chi_1, \ldots, \chi_h$. He then expressed the second orthogonality principle without summation notation, as

$$\chi_1(\Theta) + \chi_2(\Theta) + \cdots + \chi_h(\Theta) = 0,$$

for each group element Θ. In 1896, however, de la Vallée-Poussin adopted notation S_χ for summation over characters:

> Consider ... the sum extending over all the characters, that is to say over all the systems of roots
>
> $$S_\chi \chi(n) = S_\omega \omega_1^{\nu_1} \omega_2^{\nu_2} \cdots$$
>
> ... *For every number n, the sum extending over the totality of characters satisfies*
>
> $$S_\chi \chi(n) = 0,$$
>
> *the only exception being the case where*
>
> $$n \equiv 1 \pmod{M},$$
>
> *because then all the indices are zero and one has*
>
> $$S_\chi \chi(n) = \varphi(M).$$
>
> (Poussin, 1895–1896, pp. 14–15)

It is notable that he chose a symbol distinct from the usual summation symbol, $\sum$, which he used for sums ranging over natural numbers. Nonetheless, he seems to be the only nineteenth century author to have taken summation over characters at face value.

Setting aside the orthogonality relation, let us consider the subsequent calculation, involving the L-series, where those identities are put to use. We have observed that the modern notation $L(s, \chi)$ allows us to express the dependence of an L-series on the character χ, and that the notation $\sum_\chi \overline{\chi(m)} \log L(s, \chi)$ allows us to sum over characters, but these means of expression were not available to Dirichlet. In the case of a prime modulus p, Dirichlet defined the L series

$$L_0, L_1, \ldots, L_{p-2},$$

where the index corresponds to a particular numeric parameter occurring in the algebraic expression that we now recognize as the value of the corresponding character, and

$$\log L_0 + \Omega^{-\gamma_m} \log L_1 + \Omega^{-2\gamma_m} \log L_2 + \cdots + \Omega^{-(p-1)\gamma_m} \log L_{p-2}$$

to sum over the $p-1$ many L series in the case of a prime modulus. In the case of a general modulus k, each L series has a similar denotation

$$L_{\mathfrak{a},\mathfrak{b},\mathfrak{c},\mathfrak{c}',\ldots}$$

where $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{c}', \ldots$ are a sequence of numeric parameters that appear in the algebraic expression for the general character, and the summation is denoted by

$$\sum \Theta^{-\alpha_m \mathfrak{a}} \Phi^{-\beta_m \mathfrak{b}} \Omega^{-\gamma_m \mathfrak{c}} \Omega^{-\gamma'_m \mathfrak{c}'} \cdots \log L_{\mathfrak{a},\mathfrak{b},\mathfrak{c},\mathfrak{c}',\ldots}$$

where the summation ranges over the $\varphi(k)$ many choices of values of $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{c}', \ldots$. Thus Dirichlet took the L series to depend on particular tuples of numeric parameters involved in the definition of the characters, and took summations to range over these parameters. Dedekind's 1863 presentation followed Dirichlet in this respect, as did de la Vallée-Poussin's 1897 presentation. Hadamard in 1896 and Landau in 1909 adopted a tack similar to Weber's, assigning arbitrary indices to the characters, and then letting the L-series depend on those indices. For example, Hadamard wrote $\psi_1, \psi_2, \ldots, \psi_{\varphi(k)}$ for the list of characters modulo k, and defined the L-functions as follows:

$$L_\upsilon(s) = \sum_{n=1}^{\infty} \frac{\psi_\upsilon(n)}{n^s}.$$

The key summation over the characters is then written $\sum_\upsilon \frac{\log L_\upsilon(s)}{\psi_\upsilon(m)}$.

To the modern eye, it seems strange to assign otherwise meaningless indices to the characters in order to express the functional dependence of the L series on a character and to sum over them, when one can just write $L(s, \chi)$ and $\sum_\chi$. But while it was perfectly natural in the nineteenth century to sum over integers, summing over the functions themselves may not even have occurred to these authors. It is not until 1897 that we first see L series expressed as a functional dependence on characters, when de la Vallée Poussin introduced the notation $Z(s, \chi)$. Subsequent authors adopted the notation $L(s, \chi)$, reverting back to Dirichlet's use of the letter L. By 1927, for example, Landau was using $L(s, \chi)$ and $\sum_\chi$ just as we do today, and from then on the usage seems to have stuck.

6.3. Extensionalization. Let $f(x)$ be the function on the real numbers defined by $f(x) = 3x^2 + 1$. In logical parlance, the *intension* of this last expression is the manner of presentation, in some sense—if not the purely syntactic string of symbols, something close to it. In contrast, the *extension* is the abstract object denoted, that is, the abstract input–output relation. Today, when we refer to functions, we generally have their extensions in mind. A note of intensionality creeps in when we say things like "the leading coefficient of f" or "the constant term of f," but when called on to explain what we mean, we are generally able to clarify the fact that by "f" we really mean the expression for f rather than the object itself. The extensional nature of the function concept is embodied in the fact that when we define a functional $F(f)$ on a collection of functions, we ensure the definition does not depend on the manner of presentation of f, since F is supposed to "act" on the extension, not the intension.

In "Concept," we argued that this distinction was not as clearly drawn in the nineteenth century treatment of functions. Early instances of functions—not just functions on the real and complex numbers, but also objects like permutations, automorphisms, and so on—were more tightly associated with a manner of expression. The history of the treatment of characters in Dirichlet's theorem shows exactly this sort of ambiguity, and a gradual move towards an extensional treatment.

Consider, for example, the definition of the concept of character itself. For each k, the set of characters modulo k can be defined extensionally, as the set of nonzero homomorphisms from $(\mathbb{Z}/k\mathbb{Z})^*$ to the complex numbers, or intensionally, as functions defined by certain algebraic expressions involving certain primitive elements modulo the prime powers occurring in the factorization of k, and certain complex roots of unity. Even though the two definitions give rise to the same set of characters, proofs can differ in the extent to which they rely on the specific representations or the abstract characterizing property. Dirichlet's proof relied only on the symbolic representations, but we have seen that later proofs emphasized the key properties of the characters, which were extensional in nature.

Recall also that Dirichlet divided the L series into three classes, depending on a corresponding division of the characters on which they depend. Dirichlet described the division in terms of the tuples of roots appearing in the algebraic expressions, whereas a modern characterization describes the three kinds of characters as follows:

1. the character with constant value 1
2. the (other) real-valued characters
3. the (other) complex-valued characters

What is perhaps surprising is that even as later authors introduced notation like χ or ψ_i to range over characters, they still carried out the classification in terms of the roots. For example, both Dedekind's and Hadamard's division of the characters into the trivial, real, and complex cases was also described in terms of the characters' representations, even though the distinction is naturally expressed in terms of the values they take. Kronecker and de la Vallée-Poussin provided both descriptions, and even though Kronecker made it clear that all operations and classifications can be carried out, algorithmically, in terms of the canonical representations, his careful choice of notation and organization made the extensional properties salient. By 1927, Landau clearly favored the extensional characterization in his textbook.

As yet another means of highlighting the difference between intensional and extensional ways of thinking about functions, we will close this section by noting that a number of the authors we considered adopted a strikingly similar means of describing identities parameterized by the characters. Recall that after stating the generalized version of the Euler product identity (8), Dirichlet wrote:

> The general equation, in which the different roots $\theta, \varphi, \omega, \omega', \ldots$ can be combined with one another arbitrarily, clearly contains K-many particular equations.

The notion of a single identity "containing" K-many particular equations sounds strange to us today. In contrast to thinking of an identity like $e^{x+y} = e^x + e^y$ as a single equation in which x and y are taken to range over the real or complex numbers, it is almost as though Dirichlet conceived of the generalized Euler product formula as a *template*, or a *schema*, for the particular assertions obtained by instantiating the variables $\theta, \varphi, \omega, \omega', \ldots$ with the particular data representing each character. In a similar way, when Dedekind defined the L series in 1863, he wrote:

> Since these roots can have $a, b, c, c', \ldots$ values, respectively, the form L contains altogether $abcc' \ldots = \varphi(k)$ different particular series...

This manner of speaking persisted even after authors began using a single symbol χ to stand for an arbitrary character. For example, in 1882, Weber, after deriving a pair of identities involving an arbitrary character χ, wrote:

> Each of the formulas ... represents h different formulas, corresponding to the h different characters $\chi_1, \chi_2, \ldots, \chi_h$.

And in a very similar situation, de la Vallée Poussin wrote in 1897:

> ... this equation (E) represents in reality $\varphi(M)$ distinct ones, which result from exchanging the characters amongst themselves.

Such language suggests that, to some extent, authors thought of the act of "instantiating" a general identity involving characters at a particular character as somewhat different from instantiating a general identity over numbers at a particular number.

§7. Methodology and ontology revisited. Let us review some of the general historical trends we have discerned in the treatment of characters. Over time, authors isolated certain symbolic expressions appearing in Dirichlet's proof, viewed them as functions of an integer parameter (or equivalence class) n, and baptized them "characters." They isolated important properties of the characters and articulated them in a way that renders them independent from the rest of the proof. Collaterally, this made it possible to generalize the notion of a character on a multiplicative group of residues to the notion of a character on any abelian group.

Initially, each character was seen to be represented by a bundle of defining data, so what we now characterize as a functional dependence on the character was expressed as a dependence on the bundle of data, and a summation over the characters was expressed as a summation of a range of values of the bundle of data. But, over time, the role that the representing data had to play in the proof was diminished. Authors began to adopt notation and patterns of argumentation that suppressed that information, for example, by assigning arbitrary indices to the characters and letting expressions depend on those indices. Ultimately, authors simply began expressing functional dependences on, and summing over, the characters themselves.

Avoiding the need to refer to any particular representation of the characters meant relying instead on properties of the characters that can be expressed in terms of the values they take on suitable inputs. In other words, it amounted to adopting an extensional view of the characters, in which statements about the characters are cast purely in those terms. In contemporary proofs of Dirichlet's theorem, this is taken to the extreme when we define the set of characters as the set of nonzero homomorphisms from the group in question to the complex numbers, and carry out the proof without indicating any way of representing individual characters, let alone means of computing with them.

One might describe these changes as "merely notational," or "merely pragmatic." But dismissing them in that way belies the fact that these changes reflect a fundamentally different way of talking about, thinking about, and reasoning about the characters. And this was by no means an isolated example. As we have noted in the introduction, during the nineteenth century the treatment of other mathematical entities that we now take to be instances of sets, functions, or structures evolved in similar ways, and for similar reasons. So the history we have traced here is but one instance of a general transformation in mathematical thought, with a new conception of the basic objects of mathematics and

appropriate means of reasoning about them. It seems strange to resist seeing this as a change in ontology. (Gray (1992) nicely emphasizes this point.)

According to the model presented in Section 2, we should view the history of Dirichlet's theorem as a response to fundamental methodological pressures, as mathematicians struggled to meet both intrinsic and extrinsic mathematical goals while respecting intrinsic and extrinsic methodological constraints. As philosophers, we should not be interested so much in the historical and psychological contingencies that shaped the process, but, rather, the sense in which the outcome is rational and justified. In other words, we wish to understand the extent to which the methods of contemporary mathematics serve to achieve our mathematical goals, given some conception of those goals and what it means to do mathematics. Attention to the history can bring some of the goals and constraints to light, but then we are left to weigh their importance and assess the merits of the present solution. This is the point at which philosophical analysis must come into play.

In broad terms, here we will view mathematics as a process by which finite beings attempt to impose a useful order on the complex and varied data that confront them. The philosophical task is then to develop more refined characterizations of the mathematical process, in terms that adequately reflect the constraints we face as mathematical agents and the goals we pursue. In "Concept," we provided a detailed discussion of some of the various methodological benefits and concerns that accrue to the use of the modern function concept. Let us briefly review these here, and see what they have to tell us about the nature of mathematics.

Treating characters as objects, in all the senses described in Section 4, brings a number of methodological benefits. Expressions become simplified, meaning that the reader has to keep track of less information when parsing them, and the author of a proof can record and convey the relevant information more compactly. Proofs become simplified as well, meaning that readers have to keep track of less information while following the argumentative structure of a proof, and authors have to keep track of less information while working out the details. Information that is irrelevant to the argument at hand is suppressed, making key data and relationships more salient.

Moreover, proofs became more modular, as properties of the characters were abstracted away and proved separately. This further supports the aim of reducing the amount of information in play at any given point. While developing a theory of the characters, we can focus on their defining properties, and when checking that particular instances of functions are characters, we only need to check that these instances satisfy the defining properties. Then, when reasoning about these particular characters, we can invoke results from the general theory, such as the orthogonality lemma, as "black boxes." The fact that extraneous information has been filtered out means that expressions depend on fewer parameters, and inferences depend on fewer assumptions. This makes it easier to check details and avoid mistakes.

Modularity brings additional benefits, in that definitions and theorems that have been abstracted away from the body of the proof can be reused elsewhere. The process of abstraction clarifies the data that serves to parametrize a definition and the hypotheses that are required to establish a proposition. This facilitates not only using the definitions and proposition in other contexts, but also modifying the definitions and propositions by varying the parameters and hypotheses accordingly. In this way, modularity supports generality as well as reuse.

Thus, with a modular structuring, dependencies between mathematical components are minimized, and the mathematics becomes easier to understand. It also becomes easier to

ensure correctness, and components can be modified and reused. Notice, incidentally, that these are exactly the benefits associated with modularity in software engineering.[8]

The key point is that treating characters as objects supports this modularity. To start with, identifying characters as "things" means that they can be objects of study. We can make assertions about them, and specify predicates and functions that take them as arguments. Moreover, notations, definitions, and theory designed to handle other "things" now apply: we can form sums that range over the characters and reason about them; we can form sets and sequences of characters and reason about them; we can consider groups of characters and reason about them; and so on. In short, all of methods that are available to us for reasoning about mathematical objects become applicable to reasoning about characters.

Given the apparent benefits of treating characters as full-blooded objects, why did it take so long for the mathematical community to do so? When we look back at the history of mathematics, it is hard to appreciate the difficulties that accompany significant shifts in method, but they are substantial. Mathematics is a communal activity: when a mathematician writes a proof, his or her intention is that others will read it and judge it to be informative and correct. This requires that the author and the reader have a common understanding not only as to what is permissible, but also as to what is appropriate and desirable.

In Section 2, we enumerated some of the concerns that arise when new methods are introduced. In "Concept," we explored the way these concerns apply specifically to the modern treatment of characters, and to functions more generally. To start with, it is important that the new manner of speaking about functions come with clear rules of use. If there is no agreement as to which inferences are permissible—for example, under what conditions it is legitimate to consider two expressions denoting functions as "equal," and to substitute one expression for another in a given context—then the mathematical enterprise falls apart, and mathematicians cannot read each others' proofs.

Moreover, whether the rules of use are presented explicitly or implicitly, there is also the question as to whether they are consistent. Even if we think of the new treatment of characters as a mere short cut to establishing Dirichlet's theorem, such short cuts are clearly illegitimate if they lead to false or nonsensical conclusions. It is by no means apparent that there are no hidden pitfalls in quantifying over characters, summing over characters, and treating characters as arguments to other functions. It would be mathematically reckless to adopt these devices out of sheer convenience, without some assurances that the results obtained are reliable. Frege used these very concerns to motivate his foundational project:

> The endeavor to be brief has introduced many inexact expressions into mathematical language, and these have reacted by obscuring thought and producing faulty definitions. Mathematics ought properly to be a model of logical clarity. In actual fact there are perhaps no scientific works where you will find more wrong expressions, and consequently wrong thoughts, than in mathematical ones. Logical correctness should never be sacrificed to brevity of expression. (Frege, 1904, p. 665)

As suggested in Section 2, to some extent it helps to know how the new methods can be interpreted in terms of the prior methods, bolstering the understanding that *if* we try to view talk of characters as short cuts to proving new theorems, the long way is still, in principle, open to us.

[8] This is a topic is explored in greater detail in Avigad (in preparation).

Even if the new rules of use seem to be reliable, there is still the question as to whether they are meaningful. We argued in Section 6 that early authors tended to think of characters as symbolic expressions of a certain kind, or at least, as entities with canonical representations as such symbolic expressions. If the new methods no longer support such a view, one has to come to terms with the question of how one *should* think of a character. Put succinctly, once we have proved a statement about characters, what do we know?

And even if we come to believe that a certain manner of working with characters is consistent, legitimate, and meaningful, there is still the question as to whether it constitutes *good mathematics*, which is to say, whether it furthers our epistemic goals and provides satisfactory answers to our questions. This issue becomes pressing when we try to reconcile a computational conception of mathematics with the new methods of abstraction. For most of its history, mathematics was essentially computational, supplying methods of calculation that could be used to predict the motion of the planets, succeed in games of chance, and compute lengths and magnitudes of all sorts. A central feature of the modern treatment of characters is that it suppresses details of how to represent and compute with individual characters, and often even eliminates these details entirely. We may feel as though we have an understanding of what it means for a function, viewed as a general procedure, to take a natural number as input, but what does it mean for a function to take a character, viewed abstractly, as input? If we expect a mathematical theory of characters to tell us how to represent them and compute with them, then a theory that fails to provide that information is simply defective.

Separating concerns as we have done here is somewhat artificial. For example, maintaining a computational view of characters is one way of interpreting their meaning, and the ability to ascribe any sort of meaning to mathematical objects tends to clarify the rules of use and support the belief in these rules are consistent. On our analysis, the factors that ultimately support adopting a modern treatment of functions are an uneasy mix of pragmatic, empirical, and broadly philosophical considerations. That does not mean that they are not good reasons, however, nor that we have not made important philosophical progress by understanding them better.

§8. Appendix: From cyclotomy to Dirichlet's theorem. In Section 3, we sketched Dirichlet's approach to proving his theorem on primes in an arithmetic progression. Our goal here is to explain how Dirichlet is likely to have come upon his method of modifying Euler's argument to tease apart the contribution of the primes in each residue class from the overall sum of their reciprocals.

Recall that if we split up the sum in Euler's equation (2), we obtain

$$\log \sum_{n=1}^{\infty} \frac{1}{n^s} = \sum_{q \equiv 1 \bmod p} \frac{1}{q^s} + \sum_{q \equiv 2 \bmod p} \frac{1}{q^s} + \cdots + \sum_{q \equiv p-1 \bmod p} \frac{1}{q^s} + O(1). \qquad (3)$$

As explained in Section 3.2, this shows that (2) is too crude to prove Theorem 3.1: we need to know that each of the terms on the right-hand side tends to infinity, not just their sum. It is here that ideas from the theory of equations are helpful. They come into play specifically in the theory of cyclotomy from Gauss' *Disquisitiones Arithmeticae*, work with which Dirichlet was intimately acquainted. Historical overviews of the relevant ideas can be found in excellent books by Edwards and Tignol on the history of the theory of equations Edwards (1984); Tignol (2001), and Curtis' equally impressive history of representation theory Curtis (1999). Curtis also explains the role of characters in the theory of cyclotomy

and Dirichlet's proof. What we aim to do here is make the progression of ideas leading from cyclotomy to Dirichlet's proof as explicit as possible.

An important concern in the field of algebra is the extent to which the roots of a polynomial can be expressed in terms of arithmetic operations on the coefficients together with the extraction of roots. The quadratic formula dates to antiquity, and solutions to the cubic and quartic were presented by Cardano in his *Ars Magna* of 1542. A natural challenge was then to determine a similar formula for the quintic. In 1770, Lagrange presented a general method of attacking this problem, using what has come to be known as the *Lagrange resolvent*. Let $t_0, \ldots, t_{n-1}$ be the roots of the nth degree polynomial in question, and let ω be an nth root of unity, that is, a solution to the equation $\omega^n = 1$. Notice that 1 is always a solution to this equation, but there are $n - 1$ others. In fact, all of the roots can be taken to be powers a single "primitive" root of unity; for example, taking ω to be the complex number $e^{2\pi i/n}$ will do. Lagrange considered the quantity

$$t_0 + \omega t_1 + \omega^2 t_2 + \cdots + \omega^{n-1} t_{n-1},$$

as well as the quantities obtained by permuting the roots $t_0, \ldots, t_{n-1}$. Suppose ω is a primitive nth root of unity, and consider the values obtained by replacing ω in the previous expression with each of the values $1, \omega, \omega^2, \ldots, \omega^{n-1}$:

$$\begin{aligned}
x_0 &= t_0 + t_1 + t_2 + \cdots + t_n \\
x_1 &= t_0 + \omega t_1 + \omega^2 t_2 + \cdots + \omega^{n-1} t_{n-1} \\
x_2 &= t_0 + \omega^2 t_1 + \omega^4 t_2 + \cdots + \omega^{2(n-1)} t_{n-1} \\
&\vdots \\
x_{n-1} &= t_0 + \omega^{n-1} t_1 + \omega^{2(n-1)} t_2 + \cdots + \omega^{(n-1)^2} t_{n-1}.
\end{aligned}$$

Lagrange observed that one can solve for each of $t_0, t_1, \ldots, t_{n-1}$ in terms of $x_0, x_1, \ldots, x_{n-1}$. For example, consider $x_0 + x_1 + \cdots + x_{n-1}$. Summing the first column gives $n \cdot t_0$. Summing the second column gives $t_1 \cdot (1 + \omega + \omega^2 + \cdots + \omega^{n-1})$. But because ω is a root of

$$\omega^n - 1 = (\omega - 1)(\omega^{n-1} + \cdots + \omega^2 + \omega + 1)$$

and $\omega \neq 1$, we have $1 + \omega + \omega^2 + \cdots + \omega^{n-1} = 0$. Similarly, summing the third column gives $t_2 \cdot (1 + \omega^2 + \omega^4 + \cdots + \omega^{2(n-1)})$; but ω^2 is also an nth root of unity, and if ω is primitive (and $n > 2$), ω^2 is also not equal to 1, and the same argument shows that this quantity sums to 0. The same argument shows that the remaining columns also sum to 0, so we have $t_0 = (x_0 + \cdots + x_{n-1})/n$, which is the desired expression for t_0.

A similar trick works to compute the other values t_k: multiplying the ith equation by ω^{-ik} simply "rotates" the powers of ω, leaving 1's in the kth column. Thus we have

$$t_k = \frac{1}{n} \sum_{i=0}^{n-1} \omega^{-ik} x_i,$$

which provides an expression for t_k in terms of $t_0, \ldots, t_{n-1}$. Lagrange went on to consider the values of $x_0, \ldots, x_{n-1}$ that are obtained by replacing ω with other roots of unity, and conditions under which one can solve for those values, and hence $x_0, \ldots, x_n$, in terms of radicals. In doing so, he was analyzing and generalizing methods of solving equations developed by Viète, Tschrinhaus, and others who had come before. He showed that these

ideas can be used to account for the known solutions to the quadratic, cubic, and quartic equations.

The methods break down for the general solution to the quintic, but variations on the method can, however, be used to determine roots of *particular* polynomials. Consider, for example, the polynomial $x^n - 1$ itself. We have already noted that we have $x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \cdots + x^2 + x + 1)$. If n is not a prime number, the second term can be factored into polynomials of lower degree, until one reaches polynomials that can no longer be factored; these are called *irreducible* polynomials. The task of determining the roots of these polynomials is known as "cyclotomy," or "circle division," because the n complex roots of $x^n - 1$ are evenly spaced around the unit circle in the complex plane.

The problem can be reduced to the case where n is a prime number, which we will denote as p instead. In that case, $x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1$ is irreducible, and if α is any root of this polynomial, the other $p - 2$ roots are $\alpha^2, \alpha^3, \ldots, \alpha^{p-1}$. An expression for these roots in terms of radicals was provided by Vandermonde for the case where $p = 11$, and the general problem was taken up by Gauss in the last chapter of the *Disquisitiones*.[9] The solution involves using the Lagrange resolvent, and taking the roots $t_0, t_1, \ldots, t_{p-2}$ to be the $p - 1$ roots $\alpha, \alpha^2, \ldots, \alpha^{p-1}$, but in a particular order.

The proof involves choosing, for the prime p in question, a primitive element g modulo p. Recall from Section 3.2 that this means that the powers $g^0, g^1, \ldots, g^{p-1}$ modulo p are exactly the nonzero residues modulo p. The solution to the equation $x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1 = 0$ is obtained by considering the Lagrange resolvent

$$\alpha^{g^0} \cdot \omega^0 + \alpha^{g^1} \cdot \omega^1 + \alpha^{g^2} \cdot \omega^2 + \cdots + \alpha^{g^{p-2}} \cdot \omega^{p-2}, \tag{9}$$

where ω is a $(p - 1)$st root of unity. If we define t_i to be α^{g^i}, then this expression becomes

$$t_0 + \omega t_1 + \omega^2 t_2 + \cdots + \omega^{p-2} t_{p-2},$$

and we are in the situation analyzed above. Lagrange's tricks tell us that if we can solve for the values of this expression when ω is replaced by $1, \omega, \omega^2, \ldots, \omega^{p-2}$ in succession, we can solve for all the values of α^{g^i}, which are just the values $\alpha, \alpha^2, \ldots, \alpha^{p-1}$ written in a different order.

The reason for writing the elements α in the particular order they appear in (9) is that, when they are written in that order, it *is* possible to solve for each t_i, with an expression involving radicals. The details of the solution are not relevant to the proof of Dirichlet's theorem, but one particular aspect of the solution is. What makes the argument work is the careful pairing of α^{g^i} with ω^i, which has the effect that for each i and j, the element

$$(\alpha^{g^i})^{g^j} = \alpha^{g^i \cdot g^j} = \alpha^{g^{i+j}}$$

is paired with ω^{i+j}. Using the notion of "index" defined in Section 3.2, we can express this as follows: for any m and n, α^m is paired with ω^{γ_m}, α^n is paired with ω^{γ_n}, and α^{mn} is paired with $\omega^{\gamma_{mn}} = \omega^{\gamma_m + \gamma_n} = \omega^{\gamma_m} \omega^{\gamma_n}$. In other words, the key property used in the calculation of the roots of cyclotomic equations is that the map $m \mapsto \omega^{\gamma_m}$ is *multiplicative* on the nonzero residues modulo p.

[9] Gauss was particularly interested in the case where p is a prime number of the form $2^m - 1$, and showed that in that case, the solution enables one to carry out a geometric construction using compass and straightedge that divides the circle into p equal parts. The *Disquisitiones* hints at the solution to the general case, but both Edwards (1984) and Tignol (2001) observe that there are gaps in the presentation; a complete solution was provided by Galois.

Dirichlet's great insight is that these ideas can be applied in the number-theoretic setting at hand, using the fact that the Euler product formula holds more generally with such a multiplicative function in the numerator. In the case where the common difference is a prime number p, if we choose a primitive root g modulo p and define $t_i = \sum_{q \equiv g^i \bmod p} 1/q^s$, then equation (4) in Section 3.2 can be written as

$$\log \sum_n \frac{\omega^{\gamma_n}}{n^s} = t_0 + t_1\omega + \cdots + t_{p-2}\omega^{p-2} + O(1).$$

The derivation of this equation relies on the generalized Euler formula, which requires that the map $m \mapsto \omega^{\gamma_m}$ is multiplicative. But once we have the equation in hand, we need to only use the Lagrange trick, which is exactly what Dirichlet did. The more general case where p is replaced by an arbitrary modulus k is technically more difficult, but it builds on the same idea, combined with the behavior of the multiplicative group of residues modulo k that are coprime to k. Once again, this is something which Dirichlet was intimately familiar with, from the work of Gauss.

BIBLIOGRAPHY

Avigad, J. Modularity in mathematics, in preparation.

Avigad, J., & Morris, R. (2014). The of "character" in Dirichlet's theorem on primes in an arithmetic progression. *Archive for History of Exact Sciences*, **68**(3), 265–326.

Avigad, J., & Morris, R. Character and object (expanded version), unpublished. http://arxiv.org/abs/1505.07238.

Curtis, C. W. (1999). *Pioneers of Representation Theory: Frobenius, Burnside, Schur, and Brauer*. American Mathematical Society and London Mathematical Society, Providence, RI.

de la Vallée Poussin, C. J. (1895–1896). Démonstration simplifiée du théorèm de Dirichlet sur la progression arithmétique. *Mémoires couronnés et autres mémoires publiés par L'Académie Royale des Sciences, des Lettres et des Beaux-Arts de Belgique*, **53**.

Dedekind, R. (1932). In Fricke, R., Noether, E., and Ore, Ö., editors. *Gesammelte mathematische Werke*, Vols. 1–3. Braunschweig: F. Vieweg & Sohn. Reprinted by Chelsea Publishing Co., New York, 1968.

Dirichlet, J. P. G. L. (1837a). Beweis eines Satzes über die arithmetische Progression. *Bericht über die Verhandlungen der königlich Presussischen Akademie der Wissenschaften Berlin*. Reprinted in Dirichlet (1889), pp. 309–312.

Dirichlet, J. P. G. L. (1837b). Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält. *Abhandlungen der königlich Preussischen Akademie der Wissenschaften*, 45–81. Reprinted in Dirichlet (1889), pp. 313–342. Translated by Ralf Stefan as "There are infinitely many prime numbers in all arithmetic progressions with first term and difference coprime."

Dirichlet, J. P. G. L. (1840). Über eine Eigenschaft der quadratischen Formen. *Journal für die reine und angewandte Mathematik*, **21**, 98–100.

Dirichlet, J. P. G. L. (1841). Untersuchungen über die Theorie der complexen Zahlen. *Journal für die reine und angewandte Mathematik*, **22**, 190–194.

Dirichlet, J. P. G. L. (1863). In Dedekind, R., editor. *Vorlsesungen über Zahlentheorie*. Braunschweig, Germany: Vieweg. Subsequent editions in 1871, 1879, 1894, with "supplements" by Richard Dedekind. Translated by John Stillwell, with introductory notes, as *Lectures on Number Theory*, American Mathematical Society, Providence, RI, 1999.

Dirichlet, J. P. G. L. (1889). In Kronecker, L., editor. *Werke*. Berlin: Georg Reimer.
Edwards, H. M. (1984). *Galois Theory*. New York: Springer.
Euler, L. (1748). *Introductio in analysin infinitorum, tomus primus*. Lausannae. Publications E101 and E102 in the Euler Archive.
Frege, G. (1904). Was ist eine Funktion? In Meyer, S., editor, *Festschrift Ludwig Boltzmann gewidmet zum sechzigsten Geburtstage*. Leipzig: J. A. Barth. Reprinted in Frege (2002) and translated as "What is a function?" In Geach, P. and Black, M., editors, *Translations from the Philosophical Writings of Gottlob Frege*. Oxford: Oxford University Press, 1980.
Frege, G. (2002). In Textor, M. editor, *Funktion – Begriff – Bedeutung*. Göttingen: Vandenhoeck and Ruprecht.
Gauss, C. F. (1801). *Disquisitiones Arithmeticae*. Leipzig: G. Fleischer. Reprinted in Gauss' *Werke*, Königlichen Gesellschaft der Wissenschaften, Göttingen, 1863. Translated with a preface by Arthur A. Clarke, Yale University Press, New Haven, 1966, and republished by Springer, New York, 1986.
Gray, J. (1992). The nineteenth-century revolution in mathematical ontology. In Gillies, D., editor, *Revolutions in Mathematics*. Oxford: Oxford University Press, pp. 226–248.
Hadamard, J. (1896). Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences arithmétiques. *Bulletin de la Société Mathématique de France*, **24**, 199–220.
Hawkins, T. (1971). The origins of the theory of group characters. *Archive for History of Exact Sciences*, **7**, 142–170.
Kronecker, L. (1870). Auseinandersetzung einiger eigenschaften der klassenzahl idealer complexer zahlen. *Monatsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin*, 881–882. Reproduced in Kronecker (1968), vol. I, pp. 271–282.
Kronecker, L. (1895–1930). In Hensel, K., editor, *Werke*, vol. 1–5. Leipzig: B. G. Teubner. Reprinted by Chelsea Publishing Co., New York, 1968.
Kronecker, L. (1901). In Hensel, Kurt, editor. *Vorlesungen über Zahlentheorie*. Leipzig: B. G. Teubner.
Kummer, E. E. (1846). Zur Theorie der complexen Zahlen. *Koniglich Akademie der Wissenschaft Berlin, Monatsbericht*, 87–97. Also in *Journal für die reine und angewandte Mathematik*, **35**, 319–326, 1847, and in Kummer's *Collected Papers*, edited by André Weil, Springer-Verlag, Berlin, 1975, vol. 1, 203–210.
Landau, E. (1909). *Handbuch der Lehre von der Verteilung der Primzahlen*, vol. 1. Leipzig: B. G. Teubner.
Landau, E. (1927). *Vorlesungen über Zahlentheorie*. Leipzig: S. Hirzel.
Mach, E. (1960). *The Science of Mechanics: A Critical and Historical Account of its Development*. Translated by McCormack, T. J., La Salle, Illinois: The Open Court Publishing Co.
Mancosu P., editor. (2008). *The Philosophy of Mathematical Practice*. Oxford: Oxford University Press.
Manders, K. The Euclidean diagram. In Mancosu (2008), pp 80–133.
Morris, R. (2011). *Character and object*. Master's thesis, Carnegie Mellon University.
Quine, W. V. O. (1948). On what there is. *The Review of Metaphysics*, **2**, 21–38. Reprinted in Quine, W. V. O. (1980) *From a Logical Point of View*. Cambridge: Harvard University Press.
Quine, W. V. O. (1969). *Ontological Relativity, and Other Essays*. New York: Columbia University Press.

Tignol, J.-P. (2001). *Galois' Theory of Algebraic Equations*. New Jersey: World Scientific.
Urquhart, A. Mathematics and physics: strategies of assimilation. In Mancosu (2008), pp. 417–440.
Weber, H. (1882). Beweis des Satzes, dass jede eigentlich primitive quadratische Form unendlich viele Primzahlen darzustellen fähig ist. *Mathematische Annalen*, **20**, 301–329.
Wilson, M. (1994). Can we trust logical form? *The Journal of Philosophy*, **91**, 519–544.
Wittgenstein, L. (1989). *Wittgenstein's Lectures on the Foundations of Mathematics, Cambridge, 1939*. Chicago: University of Chicago Press.

DEPARTMENT OF PHILOSOPHY
CARNEGIE MELLON UNIVERSITY
E-mail: avigad@cmu.edu
E-mail: email@rebeccaleamorris.com