Appropriate Steps

A Theory of Motivated Proofs

Rebecca Morris
Department of Philosophy
Carnegie Mellon University
USA
2015

For my Grandad.

Abstract

While philosophers have long been interested in proofs, their primary focus has traditionally been on the justificational role that they play, and particularly on the certainty that they provide. Mathematicians throughout history, however, have expected proofs to do more than "just" establish a certain result. For example, mathematicians have especially valued proofs which are fruitful, obtained in a pure manner, or explanatory. Philosophers of mathematical practice have recently started to investigate such non-justificational aspects of proofs.

In this dissertation, I explore another desideratum taken from the practice of mathematics: that proofs be motivated. The topic of motivated proofs has received some discussion by mathematicians, most notably George Pólya, who emphasized that the steps in a motivated proof must not only be correct, but also appropriate, and recognized as such by the reader. However, the topic of motivated proofs has received almost no philosophical attention. It might be thought that this is because such a topic is not philosophically interesting and is better investigated by other disciplines such as psychology or pedagogy. However, while I encourage a highly interdisciplinary approach, I argue that the topic is philosophically interesting and requires philosophical work, even for it to be fruitfully studied from within a different discipline.

Throughout the rest of this dissertation, I undertake such philosophical work. More precisely, I address philosophical questions such as "What criteria should a proof meet to be motivated?", and "Should obtaining motivated proofs be a mathematical goal?" In addition I tackle the more practical question, "How can a poorly motivated proof be transformed into a better motivated one?"

Contents

Chapter 1

Introduction

While philosophers have long been interested in proofs, their primary focus has traditionally been on the justificational role that they play, and particularly on the certainty that they provide. Mathematicians throughout history, however, have expected proofs to do more than "just" establish a certain result. For example, mathematicians have especially valued proofs which are fruitful (Euler, 1750), obtained in a "pure" manner (Dedekind, 1872, 1888), or explanatory (Bolzano, 1837). Philosophers of mathematical practice have recently started to investigate such non-justificational aspects of proofs.[1]

In this dissertation, I will explore another desideratum taken from the practice of mathematics: that proofs be *motivated*. The topic of motivated proofs has received some discussion by mathematicians, most notably George Pólya. However, it has received almost no philosophical attention.[2] It might be thought that this is because the topic of motivated proofs fails to be philosophically interesting. After all, not everything that mathematicians do is of interest from a philosophical standpoint, and motivated proofs may appear to be something best investigated by psychology or pedagogy, for example. Nonetheless, I suggest that motivated proofs are of philosophical interest. Indeed, obtaining such proofs is taken to be a goal by the mathematical community, as I will demonstrate in section 2.1. As philoso-

[1]For the classical analysis of mathematical explanations, see (Steiner, 1978); for an analysis of mathematical understanding, see (Avigad, 2008); for discussion of issues of purity in mathematics, see (Detlefsen and Arana, 2011).

[2]David Sandborg is the only philosopher I know of who has discussed motivation. He suggests that a lack of motivation is due to arbitrariness in a proof (Sandborg, 1998). His work will be discussed briefly in section 2.3.2 and in more detail in chapter 6.

phers of mathematical practice, we should be interested in investigating and evaluating such mathematical goals, and should thus be interested in motivated proofs.

Additionally, while the topic is of interest in its own right, it is also connected to existing philosophical issues. An analysis of motivated proofs may help to illuminate issues concerning understanding and explanation. Indeed, motivated proofs, as we shall see below, promote understanding of how a proof works, and of how a result is obtained. Therefore an investigation of motivated proofs may yield insights about mathematical understanding, and understanding more generally. Further, the notion of motivation is related to the notion of explanation. However, as I shall argue, there are significant differences between motivated proofs and explanatory ones, at least as characterized in the literature. Understanding these similarities and differences may yield new insights into mathematical explanation as well.

However the topic of motivated proofs is not only philosophically interesting, it *requires* philosophical work, even if it is to be studied from within different disciplines. Indeed, while mathematicians identify certain proofs as well motivated, very few explain what they mean by this. Pólya is a notable exception, but even his account is not complete and raises further questions. Consequently, before we can seriously study motivated proofs, we need to consider the following question: "What criteria *should* a proof meet to be considered well motivated?" This is a distinctly *philosophical* question, as opposed to one that is psychological or pedagogical.

Nonetheless, an investigation into motivated proofs should be highly interdisciplinary. For while it is of philosophical interest and requires philosophical work, it is also of psychological and pedagogical interest, and could greatly benefit from empirical investigation by these disciplines. For example, once there is more clarity as to what criteria a proof should meet to be motivated, psychology and pedagogy may help us to write proofs that meet those criteria. Further, recent work being undertaken in the domain of proof search and interactive theorem proving, such as the AProS project directed by Wilfried Sieg, may yield important insights. Sieg describes some of the deep and fruitful connections between issues in proof search, philosophy of mathematics and psychology in his article "Searching for proofs (and uncovering capacities of the mathematical mind)" (Sieg, 2013).

The outline of this dissertation is then as follows. In chapter 2, I discuss mathematicians'

remarks about motivated proofs, and show that obtaining such proofs is taken by the community to be a mathematical goal. In chapter 3, I analyze a number of case studies from elementary number theory. More specifically, I examine different proofs of the same theorem, which, while similar, differ in their motivational efficacy. Thus comparing them allows me to tease out the source of these differences. I then use these case studies to develop my account of motivated proofs in chapter 4, and address the following questions: "What criteria should a motivated proof meet?"; "Why are motivated proofs beneficial?"; "Why should obtaining motivated proofs be a mathematical goal?"; "How can we ensure that we write motivated proofs?" In chapter 5, I examine a more complex historical case study: Dirichlet's Theorem for primes in an arithmetic progression. Finally, in chapter 6, I consider how motivated proofs relate to other, desirable types of proofs, such as explanatory ones.

Chapter 2

Motivating Motivation

2.1 Mathematicians on Motivation

I claimed, above, that obtaining motivated proofs is a mathematical goal. In this section, I substantiate this claim with examples from mathematical practice. My focus here will be on the mathematicians' remarks, rather than the actual mathematics or the philosophical implications. I will discuss philosophical methodology in section (2.3), present case studies in chapter 3, and offer an analysis of motivated proofs in chapter 4.

2.1.1 Carleman's Inequality

In his article "With, or without, motivation?", Pólya presents a proof of Carleman's inequality in two different ways: with, and without, motivational material. The theorem in question is the following (Pólya, 1949, 684): if $a_1, a_2, \ldots$ are real, non-negative numbers and are not all equal to 0, then the following inequality holds:

$$\sum_{n=1}^{\infty}(a_1 a_2 \ldots a_n)^{\frac{1}{n}} < e\sum_{n=1}^{\infty} a_n.$$

One key step in the proof is the introduction of an auxiliary sequence of real numbers c_i such that $c_1 c_2 \ldots c_n = (n+1)^n$. The proof then proceeds in a straightforward manner, making use of the arithmetic-geometric mean inequality. However, Pólya notes that in the

original presentation the c_i sequence appears as a mysterious "deus ex machina", and thus does not satisfy the reader. In order to remedy this, he suggests some additions which are included in the augmented proof: "What is needed is, not a complete, but an incomplete justification, a plausible provisional ground, just a hint that the step has some chances of success, in short, some heuristic motivation" (Pólya, 1949, 686).

More precisely, Pólya suggests that a (rationalized) account of discovery can often provide suitable motivation. Indeed, the exposition that constitutes Pólya's "heuristic motivation" in the augmented proof includes an account of how the proof develops, starting from a relatively natural approach not involving an auxiliary sequence, which fails. The failed strategy is still useful, however, as Pólya shows that it can be modified in a series of steps that ultimately provide a correct proof. Of the exposition, Pólya remarks "Now, we may understand how it was humanly possible to discover that definition of c_n which appeared ... as a "deus ex machina" ... And the origin of the theorem itself is elucidated." (Pólya, 1949, 690).

2.1.2 Rogers-Ramanujan Identities

The Rogers-Ramanujan identities can be stated in a variety of ways, both analytically and in terms of partitions. George Andrews and Rodney Baxter state them in terms of partitions as follows:

> *The First Rogers-Ramanujan Identity.* The partitions of n with difference between parts at least 2 are equinumerous with the partitions of n into parts of the forms $5m + 1$ and $5m + 4$.
>
> *The Second Rogers-Ramanujan Identity.* The partitions of n into parts > 1 with difference between parts at least 2 are equinumerous with the partitions of n into parts of the forms $5m + 2$ and $5m + 3$. (Andrews and Baxter, 1989, 401)

Andrews and Baxter aim to give a motivated proof of these identities by proceeding in a particular manner: by focusing on the right hand side of the identities, and tackling a question asked by Leon Ehrenpreis about the generating functions of the appropriate partitions (call them $G_1(q), G_2(q)$). Empirical investigations arising from this question lead to a hypothesis about the form of a recursive family of functions generated by $G_1(q)$ and

$G_2(q)$, and this, in turn, say Andrews and Baxter, leads naturally to a proof of the Rogers-Ramanujan identities. This approach is a reconstruction of how Baxter himself re-discovered the theorems and their proofs when working in statistical mechanics (see (Andrews and Baxter, 1989, 402)). Further, Andrews and Baxter emphasize the significance of starting with only the right hand side of the identities:

> ...starting with both sides begs the question of motivation. Our object was to start with the *one* side of the Rogers-Ramanujan identities concerning partitions into congruence classes mod 5. From there we examine a problem intrinsic to that side (Ehrenpreis's question), and we are consequently forced to consider partitions with differences at least 2 between parts. Or as we state in our introduction, "In answering this question we are led naturally to the Rogers-Ramanujan identities themselves" (Andrews, 1990, 215).

2.1.3 Expansion of e as a Continued Fraction

In his paper "A short proof of the simple continued fraction expansion of e", Henry Cohn presents "an especially short and direct variant of Hermite's proof" (Cohn, 2006, 57) that e can be expanded as a continued fraction in the following manner:

$$e = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \ldots}}}}},$$

or more succinctly as:

$$e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \ldots].$$

One of Cohn's explicit aims in presenting the proof, which makes crucial use of integral formulas, is to "explain some of the motivation" (Cohn, 2006, 57) behind it. He writes "The most surprising aspect of this proof is the integral formulas, which have no apparent motivation. The difficulty is that the machinery that led to them has been removed from the final proof. Hermite wrote down the integrals while studying Padé approximants, a context in which it is easier to see how one might think of them" (Cohn, 2006, 59). The remainder of Cohn's paper introduces the reader to Padé approximants, highlights how they

are relevant to the current proof, and shows how they suggest the introduction of the crucial, but previously mysterious, integral formulas.

2.1.4 Irrationality of π

Johann Lambert gave the first proof of the irrationality of π using continued fractions in 1767. His proof, however, was extremely long. Ivan Niven gave another proof in 1947 which was much shorter, and only made use of algebra and calculus. However, while Niven's proof had certain benefits over Lambert's, Timothy Jones found it to be lacking in motivation. Jones discusses the proof, and attempts to provide a more motivated version, in his paper "Discovering and proving that π is irrational".

Jones takes the introduction of certain functions in the proof to be the cause of its lack of motivation. These functions, and how they are used, are similar to functions Hermite used in his proof of the transcendence of e. However, as Jones remarks "To someone unsteeped in Hermite's technique the motivation for the proof must be unclear" (Jones, 2010, 556). Jones attempts to rectify this by introducing a "simplifying concept" to motivate the definition of these functions. He claims this enables him to give "... a more motivated and straightforward proof than Niven's. Using this concept, we, as it were, discover that π might be irrational and then confirm that it is with a proof" (Jones, 2010, 553).

2.1.5 Research vs Teaching

All of the examples discussed above are taken from *The American Mathematical Monthly*. As this journal publishes expository articles and has a broad audience, including students, this might be taken to suggest that mathematicians only care about motivation within teaching, as opposed to research, contexts. However, it is not at all clear that a sharp distinction can be made between these contexts. After all, mathematicians working on the cutting edge of their field still learn from reading their colleagues' papers, and students in high school or college may come to discover an already known result independently.

Further, there are plenty of cases where mathematicians judge proofs to be well (or poorly) motivated in more explicitly research focused contexts. Here are some examples:

> We give a generalization for Hajós' theorem. The proof of this generalization is simpler and the steps are better motivated than the proof of the original result. (Corrádi and Szabó, 1993, 4119)

> A secondary purpose [of this paper] is to show how the commonly used theory of sieves can be replaced by the theory of the Lusin-Sierpiński index ... and to emphasise that this leads to much more clearly motivated proofs. (Rogers, 1973, 491)

> The author gives a beautiful well-motivated proof of the complex Bott periodicity theorem using only two essential properties of the complex numbers ... and the group completion theorem. (Hastings, 1981)

> The paper contains a nicely motivated proof of these results and a full account of the necessary machinery from the theory of polynomial ideals and Chow forms. (Loxton, 1985)

2.2 Pólya and Motivation

Recall that in "With, or without, motivation?", Pólya gives a correct, but unsatisfactory, proof of Carleman's inequality, before augmenting it with motivational material. However, Pólya does not just give the proof and the additional material. Rather, he tries to isolate what is troubling about the first proof, and ultimately what a reader desires from a proof. Pólya's discussion is insightful, and I take it to provide a solid starting point for a philosophical investigation of motivation. Consequently, I'll discuss Pólya's remarks in more detail here.

After presenting the unsatisfactory proof, Pólya considers a number of complaints that a reader could make. These criticisms focus on the introduction of the auxiliary c_i sequence which Pólya labelled a "deus ex machina" (see (Pólya, 1949, 885)):

- The introduction of the c_i sequence seems arbitrary.
- It is not clear what purpose the c_i sequence serves.

- It is not clear how the c_i sequence will advance the proof.
- The reader cannot follow the author confidently after the introduction of the c_i sequence.
- The reader cannot learn how the author found the c_i sequence.
- The c_i sequence makes it hard to understand the proof.

Pólya takes complaints like these to indicate that a reader does not just want to recognize the correctness of each of the steps, but also their *appropriateness*. For Pólya, an appropriate step is one which "is essentially connected with the purpose, . . . it brings us nearer to the goal" (Pólya, 1949, 685). This is admittedly vague, but the underlying idea can be illustrated with a simple example. Consider a derivation in propositional logic which includes an unnecessary line, such as a redundant 'or-introduction', which is not used anywhere else in the proof. Though such a line would technically be correct, it would be objectionable as it would make no contribution to the argument—it could be removed and the proof would go through just fine. Thus, such a line would fail to be appropriate.

However, Pólya is concerned not only with the steps being appropriate; he is concerned with the reader *recognizing* their appropriateness. Indeed, he says the introduction of the auxiliary c_i sequence *is* appropriate, but it is problematic because the proof does not help the reader to *recognize its appropriateness* (see (Pólya, 1949, 686)). As Pólya explains more generally:

> It is not enough, however, that a step *is* appropriate: it should *appear so* to the reader. If the step is simple, just a trivial, routine step, the reader can easily imagine how it could be connected with the aim of the argument. If the order of presentation is very carefully planned, the context may suggest the connection of the step with the aim. If, however, the step is visibly important, but its connection with the aim is not visible at all, it appears as a "deus ex machina" and the intelligent reader or listener is understandably disappointed (Pólya, 1949, 685).

Thus the general idea behind Pólya's remarks is as follows: for a proof to be motivated, not only must the steps be correct, and recognizably so, they must also be appropriate and recognized as such by the reader. Although he does not provide much in the way of further elaboration of these remarks, they do appear to fit the examples briefly discussed in section 2.1. In Pólya's own example, the additional motivational material helps the reader to recognize that the introduction of the c_i sequence is appropriate by showing her how it "fixes up" a natural, but unsuccessful, strategy. Andrews and Baxter purposefully work with only one side of the Rogers-Ramanujan identities to help their proof arise in a "natural" manner, which will presumably make it easier to recognize the appropriateness of the steps compared to a convoluted or artificial proof. By introducing the reader to Padé approximants, and showing how they are relevant to the proof, Cohn helps the reader to better grasp how the mysterious functions contribute to the argument, and thus recognize their appropriateness. Finally, Jones' "simplifying concept" is intended to help the reader grasp the role of the mysterious-looking functions in his proof, thus helping her to recognize their appropriateness.

Consequently, Pólya's remarks form a suitable starting point for a deeper, more philosophical, analysis of motivation.

2.3 Prelude to an Analysis of Motivated Proofs

2.3.1 The Project

As seen above, mathematicians value motivated proofs, though they do not, on the whole, explain what such proofs are or why they are desirable. Pólya goes further in this regard, though his discussions in "With, or without, motivation?" are still brief and prompt further questions. For example, although he emphasizes that the reader of a proof wants to recognize not just the correctness, but also the appropriateness, of the steps, he doesn't identify how a step may (fail to) be recognized as appropriate. The situation thus seems ripe for philosophical investigation: mathematicians have identified a valuable property some proofs possess while others lack (being motivated), though they have not identified precisely what

this amounts to or why it is beneficial.

However, in undertaking a philosophical analysis of motivated proofs, I am *not* investigating how mathematicians use the phrase "motivated proof". Rather, my task is to tackle questions such as: "What criteria should a proof meet if it is to be called motivated?"; "Should obtaining motivated proofs be a mathematical goal?"; "How can a poorly motivated proof be transformed into a better motivated one?"; "How can mathematicians write better motivated proofs?".

I will use case studies to help answer these questions by comparing different proofs of the same theorem. In most cases, the proofs will be very similar, though the small differences have a significant impact on their pre-theoretical motivational efficacy. This will allow me to identify concretely what is responsible for the change in motivational efficacy. The case studies also have a historical component: I will often compare older proofs with their more modern counterparts. In many cases, the modern proofs are (pre-theoretically) better motivated than the historical ones. However, this is *not* meant as a criticism of the older proofs. Rather, it reflects the fact that, when trying to prove a new result, the most important goal is to obtain a correct proof; motivation is a secondary consideration, albeit an important one. Further, as shall become clear, motivating a proof can take a considerable amount of work.

2.3.2 Connections to Other Topics

While I am framing this as an investigation of "motivated proofs", I am not strictly wedded to the terminology. That is to say, if someone would rather call my account of motivated proofs an account of proofs with property X, I would be open to the suggestion. Nonetheless, I maintain that "motivated proofs" is a suitable name, given that my analysis builds on Pólya's discussion. The crucial point about my analysis, however, is not the name of the property, but the property itself, the benefits it brings, and how to ensure that proofs possess it. This is not something that, to my knowledge, has been identified and subjected to a philosophical study.

As mentioned in the introduction, the topic of motivated proofs connects to theories of understanding and explanation. There has been considerable philosophical interest in

mathematical explanation and related topics, such as non-arbitrariness, and it might be thought that a motivated proof is nothing but an explanatory or non-arbitrary proof. For example, it might be suggested that Pólya's emphasis on recognizing the appropriateness of steps in a proof is another way of stressing the importance of explanatory proofs, or of ensuring that the steps in a proof do not appear arbitrary. However, this is not an accurate assessment. I will give a careful comparison of my account of motivated proofs and the standard literature on mathematical explanation and non-arbitrariness in chapter 6. However, for now I will briefly discuss explanatoriness and non-arbitrariness, and suggest that the class of motivated proofs is not necessarily the same as the class of explanatory or non-arbitrary proofs.

First, it is not at all clear what is meant by "explanatory proof". Intuitions vary wildly as to which proofs are considered "explanatory" and which are not. As Marc Lange remarks "Philosophers disagree sharply about which proofs of a given theorem explain *why* that theorem holds and which merely prove *that* it holds" (Lange, 2009, 203). Thus, if someone proposes that Pólya's remarks can be understood in terms of explanation, it is not entirely clear what (s)he means. However, there are two well-known accounts of mathematical explanation that may be appealed to, which were developed by Philip Kitcher (Kitcher, 1989) and Mark Steiner (Steiner, 1978).[1]

Although Kitcher's main focus is *scientific* explanation, he claims that his theory also applies to mathematics (see (Kitcher, 1989, 437)). Central to his theory of explanation is the notion of *unification*. Very roughly, Kitcher's account claims that explanatory proofs in a domain K are those which belong to the "explanatory store", $E(K)$, for K (Kitcher, 1989, 430–434). $E(K)$ is the set of derivations which constitute the best, i.e. most unifying, systematization of mathematical beliefs about K. Judgements about the degree to which a systematization is unified can be made by reference to the argument "patterns" that generate the derivations in the systematization under consideration. More precisely, the most unifying systematization is the one that allows the most conclusions to be drawn from the fewest number of patterns, assuming that the patterns are not gerrymandered (see (Kitcher, 1989,

[1]These two accounts of mathematical explanation have been widely discussed in the literature. See for example (Resnik and Kushner, 1987), (Hafner and Mancosu, 2005), (Hafner and Mancosu, 2008a) and (Frans and Weber, 2014).

432–434)). Thus, for Kitcher, a proof is only explanatory in virtue of its inclusion in the most unifying systematization for the mathematical domain.

Steiner adopts a quite different approach. In particular, he identifies two criteria for an explanatory proof: (i) the proof invokes a "characteristic property" of something mentioned in the theorem and is clearly dependent on this property (see (Steiner, 1978, 143)); (ii) the proof is generalizable, in the sense that varying the characteristic property yields a proof of a new but related theorem (see (Steiner, 1978, 147)).

Pólya's discussion of motivated proofs points to qualities quite different from those captured by Kitcher's and Steiner's accounts of explanation. Take Kitcher's theory first. A proof is explanatory on his account if it belongs to the explanatory store for the relevant domain. In other words, such a proof instantiates argument patterns that generate the explanatory store. However, this is very different in focus from Pólya's remarks. To be motivated, according to Pólya, a proof must be such that a reader can recognize the correctness and appropriateness of the proof steps (assuming the steps are, indeed, correct and appropriate). Yet it seems reasonable to suppose that an argument pattern in the explanatory store can be instantiated in a strange or unusual way, one which gives the reader pause and raises further questions. This suggests that there may be proofs that are explanatory according to Kitcher's theory but which are not well motivated. Further, at least prima facie, it seems possible for there to be proof steps which are recognized as appropriate by the reader, but which fail to be part of an instantiation of an argument pattern that belongs to the explanatory store. Otherwise, the only steps that a reader can recognize as appropriate are those which form part of the "best" systematization of the domain, which seems an artificial restriction. Consequently, it seems possible for there to be motivated proofs which fail to be explanatory according to Kitcher's theory. Thus Kitcher's notion of an explanatory proof seems quite distinct from a pre-theoretical notion of motivated proof.

Steiner's account of explanation also appears different from Pólya's remarks on motivated proofs. Recall that, for Steiner, an explanatory proof clearly depends on a "characterizing property" of an entity in the theorem, and further is generalizable. However, it is quite possible for a proof to exploit such a "characterizing property" in a weird or unusual way. A reader of this theorem may recognize that the proof depends on the property, and even see

how the proof can be generalized, all the while having questions about certain steps in the proof, similar to those Pólya imagined his students asking, such as: "How did the author find this step?", "What purpose does it play?" and so on. Consequently, it seems possible for there to be proofs which are explanatory but not motivated, at least according to Steiner's account of explanation. Further, there may be proofs that are motivated, but not explanatory according to Steiner's criteria. Proofs by induction may fall into this category. Take, for example, the standard proof by induction that the sum of the first n integers is $n(n+1)/2$. Assuming the reader is comfortable with the method of mathematical induction, she is likely to recognize that the steps in the argument are both correct and appropriate: there is no "deux ex machina" step.[2] However, on Steiner's account, the proof is not explanatory. He writes of this very proof: "The proof by induction does not characterize anything mentioned in the theorem. Induction, it is true, characterizes the set of all natural numbers; but this set is not mentioned in the theorem" (Steiner, 1978, 145). This at least suggests that there are differences between Steiner's notion of an explanatory proof and what I am calling a motivated proof.

There is thus some reason to suspect that motivated proofs are not the same as explanatory proofs. I now turn to non-arbitrary proofs, or proofs which contain no arbitrary steps. David Sandborg is one of the only philosophers I know of who has discussed motivated proofs in his work, and he connects a lack of motivation to arbitrariness. He discusses Pólya's unmotivated proof of Carleman's inequality and notes "... one of the steps in Pólya's proof, the introduction of the c_i sequence, appears unmotivated ... This dissatisfaction can be understood in terms of arbitrariness" (Sandborg, 1998, 143). As he explains, referring to a number of case studies, "... a proof step seemed arbitrary when we saw no reason why it was taken as opposed to some other possibility" (Sandborg, 1998, 154). Consequently, arbitrariness can be reduced by identifying a favorable property that the selected step has but which other possible steps lack. More precisely, Sandborg requires that this is done via a comparison of all of the possibilities at the same time and showing, or at least suggesting, that the selected one has the favorable property while (most of) the others lack it. Accord-

[2]While I am suggesting that a reader who has mastered the method of mathematical induction will find this proof motivated, I recognize that many students have difficulty mastering the technique.

ing to Sandborg, this requires that (i) the possibilities be represented generically; (ii) the possibilities be uniformly compared with respect to the property (Sandborg, 1998, 148–149).

Sandborg does recognize that it is not always necessary to carry out such a comparison. Steps that are "standard", for example, fall into this category, as he explains "For such steps, there may be no need to compare them with other possibilities; their appropriateness is immediately clear" (Sandborg, 1998, 152). However, I suggest that conditions (i) and (ii) are not necessary to help a reader recognize the appropriateness of a proof step much more generally. Indeed, if they were necessary, then it would be all but impossible to help the reader recognize the appropriateness of a step that utilizes an initially perplexing proof *strategy*. As Sandborg himself notes, "Proof strategies are too diverse to admit uniform comparisons" (Sandborg, 1998, 146). However, it seems that in many cases a mysterious choice of strategy *can* be made to appear appropriate to the reader. I suggest that Pólya's reasons for adopting the strategy of introducing an auxiliary sequence in his proof of Carleman's inequality are an example of this. Sandborg, however, characterizes them as "... somewhat vague, ill-defined, and unconvincing" (Sandborg, 1998, 145), precisely because Pólya could not compare his strategy with other possibilities. I will return to this disagreement in chapter 6.

Chapter 3

Elementary Case Studies

3.1 Preliminary Remarks

In this chapter, I discuss proofs of three theorems from elementary number theory:

- Difference of Two Squares theorem: Every odd integer can be represented as the difference of two squares.
- Fermat's Little theorem: If p is a prime and a an integer not divisible by p, then $a^{p-1} \equiv 1 \mod p$.
- Wilson's theorem: If p is a prime, then $(p-1)! \equiv -1 \mod p$.

In each case, I will discuss one proof which, pre-theoretically, appears unmotivated. I will analyze why this is the case, and additionally consider how it might be overcome by discussing modified, or completely new, proofs of the same theorem. This will provide data against which to deepen and sharpen Pólya's observations, by allowing me to tease out different ways in which a proof step may be appropriate and recognized as such, as well as allowing me to further test the relationship between appropriate steps and motivated proofs. In chapter 4, I bring these considerations together into a theory of such proofs.

3.2 The Difference of Two Squares Theorem

3.2.1 A Proof of the Difference of Two Squares Theorem

The Difference of Two Squares theorem, above, states the following: Every odd integer can be represented as the difference of two squares. The following is a very simple proof of this result (see for example (Erdős et al., 2003, 219)).

Proof. Let m be an odd number. Then $m = 2k + 1$. Notice that

$$\begin{aligned}&(k+1)^2 - k^2\\ &= k^2 + 2k + 1 - k^2\\ &= 2k + 1\end{aligned}$$

Thus every odd number can be represented as a difference of two squares. □

The proof is quick and easy, and anyone familiar with elementary algebra and number theory can verify its correctness. Indeed, experienced mathematicians should find the proof trivial, and perfectly well motivated. Those with less experience, however, may judge it to be unmotivated.[1] There is one step, in particular, that seems responsible for such a judgement: the selection of k and $k + 1$. However, once the reader sees the choice of these integers, she should appreciate how they advance the proof, recognizing immediately that the choice leads to a favourable algebraic form. In other words, although the reader finds the step problematic, it may not be because she fails to see how it is connected with the aim of the argument: she may thus recognize its appropriateness in Pólya's sense. In such a case, the complaint about the step likely lies elsewhere: *in failing to see where the selection comes from, or what suggests it.* This indicates that there is thus another sense in which a step may fail to be recognized as appropriate.

This lack of recognition about where a step comes from is reflected in one of the hypothetical complaints about Pólya's unmotivated proof of Carleman's inequality described in section (2.2): the reader cannot learn from the proof how the definition of the auxiliary

[1] See, for example, posts on sites such as the Mathematics Stackexchange website.

sequence was found (see (Pólya, 1949, 885)). Pólya, however, seems to connect the recognition of how a step advances the argument to recognition of what suggests it, given that he focuses on the former in his paper. Further, he endorses the following hypothetical remark about the introduction of the mysterious auxiliary sequence "This step is not trivial. It seems crucial. If I could see that it has some chances of success, or see some plausible provisional justification for it, then I could also imagine how it was invented and, at any rate, I could follow the subsequent reasoning with more confidence and more understanding" (Pólya, 1949, 685). However, in the case of the Difference of Two Squares theorem, a reader may recognize, upon seeing the selection of k and $k+1$, that they will lead to a successful proof, yet still have reservations about what suggested this choice. Thus it seems that these two senses of recognizing the appropriateness of a step can come apart.

However, the dissatisfaction that a student experiences with such a proof can be easily remedied. Again, assuming the reader is familiar with basic algebra, the following considerations will presumably be helpful (see e.g. (Papercuts), (Wick)):

Motivational Material 1

To see how k and $k+1$ are chosen, we reason as follows (see e.g. (Papercuts)). We want to find integers x and y such that:

$$2k+1 = x^2 - y^2.$$

We can then rewrite this as follows:

$$2k+1 = (x-y)(x+y).$$

Now, to try to make the left hand side of the above equation look more like the right hand side, we can again rewrite it as:

$$1 \cdot (2k+1) = (x-y)(x+y).$$

At this point, we make a guess to see if we can get further and try setting $x-y=1$ and $x+y=2k+1$. Then we have a pair of simultaneous equations in two unknowns. Moreover,

we find that they are solvable, yielding $x = k + 1, y = k$.

Motivational Material 2

Another way to see how k and $k + 1$ are selected is to reason in the following way, which is very similar to the argument presented in 'Motivational Material 1'. We want to represent $2k+1$ as a difference of squares. But this time, instead of using x and y, we write x as $y+w$, where w is a natural number. Then we have the following:

$$\begin{aligned} 2k + 1 &= (y + w)^2 - y^2 \\ &= y^2 + 2yw + w^2 - y^2 \\ &= 2yw + w^2 \\ &= w(2y + w) \end{aligned}$$

We can try to simplify things by setting $w = 1$. This then yields the equation $2k+1 = 2y+1$. Thus we can set $y = k$ and $x = k + 1$.

Motivational Material 3

Yet another way to help motivate the proof would be to show the reader some mathematical experimentation. For example, in trying to represent some small odd numbers as a difference of two squares, we find[2]:

$$\begin{aligned} 1 &= 1^2 - 0^2 \\ 3 &= 2^2 - 1^2 \\ 5 &= 3^2 - 2^2 \\ 7 &= 4^2 - 3^2. \end{aligned}$$

Having seen some mathematical experimentation, the reader can discern a pattern: the odd numbers can be represented as a difference of consecutive squares, and, in general, if our

[2]In this case, all the numbers we are experimenting with, except 1, are prime. This is relevant because while the representation of odd primes as a difference of two squares is unique, this is not true for odd numbers generally. For example, $57 = 11^2 - 8^2 = 29^2 - 28^2$.

odd number is $2k + 1$ then $2k + 1 = (k + 1)^2 - k^2$. This is, of course, only a conjecture at this stage, but it shows the reader how the choice of k and $k+1$ could have been arrived at.

Motivational Material 4

A further way to motivate the proof would be to change the statement of the theorem itself. For example, if the theorem is sharpened to state "Every odd integer can be represented as the difference of two *consecutive* integers", the choice of k and $k + 1$ will no longer appear mysterious; they are immediately suggested by the statement of the theorem.

3.2.2 Discussion of the Difference of Two Squares Theorem

This example highlights three important points which will be further developed by examining more complex case studies. The first is that whether a proof is motivated or not depends on the context it is evaluated against. As mentioned above, an experienced mathematician, who is assessing the proof with respect to a rich, sophisticated context, will likely find the proof of the Difference of Two Squares theorem perfectly well motivated. Students, on the other hand, who are evaluating the proof with respect to a much more limited context, may judge the proof to be unmotivated. Pólya seems to have recognized this, given that he made remarks such as these: "If the order of presentation is very carefully planned, the context may suggest the connection of the step with the aim" (Pólya, 1949, 685); "An alert teacher should be able to find out how much stress on motivation suits his audience, how much suits himself personally, and how much time he has for motivation" (Pólya, 1949, 690). In other words, not only will the context impact judgments of motivation, it should also be taken into account when considering how to improve the degree to which a proof is motivated.

However, this notion of context dependence must be sharpened. Indeed, while I have asserted its importance, I have neither spelled out how the context is to be understood, nor how it impacts judgments of motivation. Certainly the context should include the mathematical tools with which a reader is assumed to be familiar, for example certain definitions, techniques, theorems, proofs and heuristics. However, as shall become clear later on, how these tools are arranged and "fit together", is also important. Thus a context is *not* conceived of as a deductively closed set of propositions, but rather as more of a toolbox, which

is structured to help organize the tools it carries, and to help the craftsman access them easily. The further case studies I examine in the remainder of this chapter will help to bring this notion of context dependence into sharper focus.

The second important point is that there is an additional sense of appropriateness that can impact whether a proof is motivated or not. As was mentioned above, the problematic step in the proof of the Difference of Two Squares theorem is the selection of k and $k+1$, but this is not because the reader fails to recognize their contribution to the proof. Rather, it is because the reader does not recognize where they come from, or what suggests their selection. And, just as Pólya drew a distinction between a step *being* appropriate (in his sense) and being *recognized* as appropriate (in his sense), such a distinction must be made for this new notion of appropriateness. To distinguish between Pólya's notion of appropriateness and the 'new' notion, let's refer to Pólya's notion as *contribution appropriateness*, and the 'new' notion as *introduction appropriateness*. Then a step will be *introduction appropriate* if it is "suggested by" the context. A reader situated in the context will be said to recognize that a step is introduction appropriate if she can, for example, answer questions such as "Where does that step come from?", "What suggested introducing that step?" Again, this needs further sharpening, which an analysis of additional case studies will provide.

The final important point that I wish to draw attention to is this: there are often multiple ways to help increase the degree to which a proof is motivated. Indeed, I discussed four different ways that the proof of the Difference of Two Squares theorem could be improved from the point of view of motivation. This may make it seem as though attempts to increase the motivational value of a proof will have to be ad hoc, with very few general strategies. However, this is not the case, and I will discuss general strategies that can be appealed to in chapter 4.

3.3 Fermat's Little Theorem

Recall that, in modern terminology, Fermat's Little theorem can be stated as follows: If p is a prime and a an integer not divisible by p, then $a^{p-1} \equiv 1 \mod p$. Leonhard Euler was the first mathematician to publish a proof of this theorem in his 1736 paper "Theorema-

tum quorundam ad numeros primos spectantium demonstratio" (Euler, 1741). Many other proofs followed, including one due to James Ivory in 1806.[3] Ivory believed his proof to have certain virtues over Euler's, as he explains at the start of his paper "I believe the following demonstration to be new and I reckon it is more simple than that of Euler" (Ivory, 1806, 6). In this section I will discuss two proofs of Fermat's Little theorem that use Ivory's argument: the first is Ivory's original proof, the second is inspired by Dirichlet-Dedekind's proof of a generalization of the theorem. Before examining the case studies in detail, however, it will be useful to summarize the main points of the argument.

Sketch of Core Argument

The key idea of the argument is to consider the sequence $a, 2a, 3a, \ldots, (p-1)a$. Considered mod p and ignoring ordering, this sequence is the same as $1, 2, 3, \ldots, (p-1)$. This means that the products of these sequences will be equal, i.e. $a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \mod p$. Rearranging yields $a^{p-1}(p-1)! \equiv (p-1)! \mod p$. However, as $(p-1)!$ is not divisible by p, we can cancel $(p-1)!$ from both sides to yield $a^{p-1} \equiv 1 \mod p$, and thus the result is proved.

3.3.1 Ivory's 1806 Proof

The modern congruence notation used in the statement of Fermat's Little theorem was first introduced by Carl Friedrich Gauss in his *Disquisitiones Arithmeticae* of 1801. However, Ivory did not use congruence notation, and thus his statement of the theorem, and his proof, looks quite different to modern versions. Ivory stated the theorem as follows: "Let p be any prime number, and N any number not divisible by p, then $N^{p-1} - 1$ will be divisible by p" (Ivory, 1806, 7).

In order to follow Ivory's argument, the reader needs to be familiar with only elementary algebra and number theory. In particular, the reader should be able to perform simple algebraic manipulations, such as rearranging equations and expanding polynomials, and recall the definition and key properties of prime numbers, such as Euclid's lemma, which states that if p is a prime and p divides a product ab then either p divides a or p divides

[3] For full details of the history of Fermat's Little theorem, see e.g. (Dickson, 2012, 59–104).

b. In addition, the reader should be familiar with results about division, in particular the Euclidean algorithm, which establishes that if a and $b > 0$ are integers, then there are unique integers q and r such that $a = qb + r$ where $0 \leq r < b$.

Ivory's first step was to consider the sequence $N, 2N, 3N, \ldots, (p-1)N$ after dividing each term by p. He argued that none of these numbers are themselves divisible by p, and that their remainders must all be different:

> That none of the multiples are divisible by p is very evident: for if $m \times N$ be one of them, p does not divide N by hypothesis, and m is less than p; therefore, p cannot divide the multiple $m \times N$. I likewise say, that the several remainders are all different from one another. For if it be possible let $m \times N$ and $n \times N$ be two multiples that, when divided by p, have the same remainder r; then
>
> $$m \times N - r$$
> $$n \times N - r$$
>
> will be multiples of p: therefore, the difference $m \times N - n \times N = (m - n) \times N$ will likewise be a multiple of p, which is impossible, because $m - n$ is less than p, and N is not a multiple of p by hypothesis; therefore, no two of the multiples, when divided by p, can have the same remainder. (Ivory, 1806, 7)

Thus, as all of the remainders will be less than p, they must be exactly $1, 2, 3, \ldots, (p-1)$, in some order. At this point Ivory introduced a new notation:

> Let us now adopt the notation $m \cdot p$ to denote a multiple of p in general, without attaching the notion of any particular number to the symbol m. (Ivory, 1806, 7)

With this new notation in hand, he noted that the sequence $N, 2N, 3N, \ldots, (p-1)N$ can be represented in a quotient and remainder format as $m{\cdot}p{+}1, m{\cdot}p{+}2, m{\cdot}p{+}3, \ldots, m{\cdot}p{+}(p{-}1)$ in some order. Here it is important to heed Ivory's remarks about his new notation, as we cannot treat each m that occurs as having the same value. As these two sequences are equal,

Ivory equated their products to obtain the following:

$$N \times 2N \times 3N \ldots \times (p-1)N = \\ (m \cdot p + 1) \times (m \cdot p + 2) \times (m \cdot p + 3) \ldots \times (m \cdot p + (p-1)).$$

Next, Ivory expanded the product on the right-hand side. He reasoned as follows:

> Now, if the expression on the right-hand side of the equation be evolved, it will consist of a certain number of terms, all of which, excepting the last, will contain p or some power of p, as a factor; and the last term will be the continued product of all the numbers less than p: let the last term be denoted by Q, then it is clear that the right hand side of the equation may be represented by $m \cdot p + Q$ ... (Ivory, 1806, 8)

As the left hand side of the equation can be written as $QN^{(p-1)}$, Ivory substituted these newly obtained representations in for the left and right hand side of the equations and rearranged them as follows:

$$QN^{(p-1)} = m \cdot p + Q.$$

Hence:

$$Q(N^{(p-1)} - 1) = m \cdot p.$$

Thus, as p is a prime, this means that p must divide Q or $N^{(p-1)} - 1$. However, as Q is the product of positive integers less than p, p cannot divide Q. Consequently p must divide $N^{(p-1)} - 1$, which proves the theorem.

3.3.2 A Dirichlet-Dedekind Style Proof

A more modern presentation of a generalization of Fermat's Little theorem can be found in the *Vorlesungen über Zahlentheorie*, a textbook based on lectures by Lejeune Dirichlet, edited and expanded by Richard Dedekind, first published in 1863. The proof that I'll give

below is based on that argument, but is restricted to the special case of Fermat's Little theorem.

In order to follow the Dirichlet-Dedekind style proof, the reader must be familiar with more sophisticated mathematics than is required for following Ivory's original proof. In particular, the reader must be familiar with modular arithmetic, including the law of cancellation, which states that if $(a, n) = 1$ then $a \cdot b \equiv a \cdot c \mod n \Rightarrow b \equiv c \mod n$. The reader will also need to know an additional concept and an extra lemma. The additional concept is that of a reduced residue system (see e.g. (Andrews, 2012, 54)):

Definition Let $m > 0$ be an integer. Then a *reduced residue system* mod m is a set of integers $R := \{r_1, \ldots, r_n\}$ satisfying the following conditions:

1. Each r_i in R is coprime to m, i.e. for each $1 \leq i \leq n$, $(r_i, m) = 1$.

2. For any $r_i, r_j \in R$, if $r_i \equiv r_j \mod m$ then $i = j$.

3. For any integer s coprime to m, there is some $r_t \in R$ such that $s \equiv r_t \mod m$.

More concisely, $R := \{r_1, \ldots, r_n\}$ is a reduced residue system mod m iff, for each s coprime to m, there is exactly one $r_t \in R$ such that $s \equiv r_t \mod m$. As an example, if m is a prime p, then $\{1, 2, \ldots, (p-1)\}$ is a reduced residue system mod p.

Remark A reduced residue system mod m has $\phi(m)$ elements, where $\phi(m)$ is the Euler phi-function, and is defined as the cardinality of the following set: $\{n : 1 \leq n \leq m \text{ and } (n, m) = 1\}$. In particular, if m is a prime p then $\phi(m) = p - 1$.

The additional lemma that the reader must know is about reduced residue systems. The following formulation is taken from the *Vorlesungen* (Stillwell, 1999, 24), but modified to apply to reduced, rather than complete, residue systems. Of the result, Dirichlet-Dedekind remarked that it "... is of particular importance in later investigations" (Stillwell, 1999, 24).

Lemma 3.3.1. *If a is relatively prime to the modulus k and if one replaces x in the expression ax by the series of all terms in a reduced residue system mod k, then the resulting values also form a reduced residue system mod k.*

Proof. Let $X := \{x_1, \ldots, x_{\phi(k)}\}$ be our reduced residue system, and let $aX := \{ax_1, \ldots, ax_{\phi(k)}\}$. Then as $(a, k) = 1$ and as $(x_i, k) = 1$ for each $1 \leq i \leq \phi(k)$, we must have that $(ax_i, k) = 1$ for each $1 \leq i \leq \phi(k)$. Hence (i) is satisfied. Further, because of the law of cancellation, $ax_i \equiv ax_j \mod k \Leftrightarrow x_i \equiv x_j \mod k$. Thus as X is a reduced residue system, $ax_i \equiv ax_j \mod k$ if and only if $i = j$ and (ii) is satisfied. Finally, as aX has $\phi(k)$ distinct elements that are all incongruent mod k, we know that it must contain a representative for each equivalence class mod k. This means that for any integer s coprime to m, there is some $ax_j \in aX$ such that $s \equiv ax_j \mod k$ and thus (iii) is satisfied. □

Remark Notice that lemma (3.3.1) means that, considered mod k, the reduced residue system $\{ax_1, ax_2, \ldots, ax_n\}$ is a permutation of the original reduced residue system $\{x_1, x_2, \ldots, x_n\}$.

Now I'll present the Dirichlet-Dedekind style proof of Fermat's Little theorem. Recall that the result to be proved states that if a is not divisible by p then $a^{p-1} \equiv 1 \mod p$.

Dirichlet-Dedekind began by considering ax as x runs through the reduced residue system $\{1, 2, \ldots, (p-1)\}$. By lemma (3.3.1), this will yield another reduced residue system. Hence we can set

$$\begin{aligned} 1a &\equiv b_1 \mod p \\ 2a &\equiv b_2 \mod p \\ &\ldots\ldots \\ (p-1)a &\equiv b_{p-1} \mod p \end{aligned}$$

where $b_1, b_2, \ldots, b_{p-1}$ is just a permutation of $1, 2, \ldots, (p-1)$. Hence if we multiply the above $p-1$ congruences, we obtain:

$$1a \cdot 2a \cdot \ldots \cdot (p-1)a \equiv b_1 \cdot b_2 \cdot \ldots \cdot b_{p-1} \mod p.$$

Hence

$$a^{p-1}(p-1)! \equiv (p-1)! \mod p$$

and hence, via cancellation,

$$a^{p-1} \equiv 1 \mod p.$$

Thus the theorem is proved.

3.3.3 Discussion of Proofs of Fermat's Little Theorem

Analysis

As I have stressed above, the context against which a proof is evaluated will impact the degree to which it is motivated. Although I have not yet clarified what is meant by "context", the intuitive understanding as a "mathematical toolbox" that a reader has at her disposal will serve as a starting point. In what follows, then, I will evaluate Ivory's original proof, as well as Dirichlet-Dedekind's more modern presentation, with respect to a minimal context. By "minimal" here I mean a context that at least provides the reader with enough mathematics to verify the correctness of each of the steps, but potentially does not go beyond this. The minimal context I will assess Ivory's proof against is less sophisticated than the minimal context I'll use for Dirichlet-Dedekind's proof. This is necessary, as Dirichlet-Dedekind's proof explicitly involves concepts and invokes lemmas that are not needed to follow Ivory's proof. However, later I will also consider both Ivory's proof and Dirichlet-Dedekind's proof from a common context. Throughout I will be particularly interested in whether the steps in the arguments are appropriate and whether they should be recognized as such by the reader.

The minimal context that I'll evaluate Ivory's proof against consists of elementary algebra and elementary number theory, as discussed in section (3.3.1). Recall there that I highlighted that the reader needed to be familiar with Euclid's lemma and the Euclidean Algorithm. The minimal context against which I'll consider Dirichlet-Dedekind's presentation consists of elementary algebra, as well as modular arithmetic. Recall that in section (3.3.2) I indicated a reader needed to know modular arithmetic, and, in particular, be familiar with the cancellation law, as well as the notion of a reduced residue system, and lemma (3.3.1). Notice also that lemma (3.3.1) is identified by Dirichlet and Dedekind as a particularly important result. This will be significant later on. Later, when evaluating both proofs with respect to the same context, I will take the "union" of individual "minimal" contexts just

described.

Pre-theoretically, I suggest that Ivory's proof fails to be well-motivated when considered against its minimal context, as it raises questions that the reader cannot answer. In particular, even after completing the proof, the reader may question where the crucial sequence $N, 2N, \ldots, (p-1)N$ comes from. Additionally, although she should be able to identify its contribution to the argument, she should not be expected to do so immediately. Indeed, certain aspects of the proof make it more difficult for the reader to do this. The Dirichlet-Dedekind style proof, however, appears to fare better with respect to its own minimal context, given that it helps the reader to answer these questions. In particular, the reader can more easily see what suggests the introduction of the corresponding sequence, as well as the contribution that it makes to the overall argument. Thus there appears, pre-theoretically, to be a significant difference in the motivational efficacy of these two proofs, which relates to whether the steps are appropriate and recognized as such. Consequently a deeper analysis of the extent to which the steps in these proofs are appropriate, and recognizably so, will help me to clarify these notions, as well as to more concretely identify factors that can impact the motivational value of proofs.

While it may be somewhat difficult for a reader to recognize exactly how the sequence $N, 2N, \ldots, (p-1)N$ contributes to Ivory's proof, it does indeed advance the argument. In particular, the product of the terms in this sequence can be represented in a form that doesn't involve N: $(p-1)! + mp$. Equating these two representations then allows the result to be obtained via calculation. The step thus advances the argument and it is possible to give a satisfactory answer to the question "How does this step advance the proof?" within the context. However, whether a hypothetical reader should recognize this and be expected to arrive at a satisfactory answer is less clear. Indeed, there is a global feature of the proof that makes this harder for the reader: the proof's lack of modularity.[4]

Briefly, modularity describes localizing information into self-contained parts or "modules", and ensuring that irrelevant or unnecessary information is hidden. Ivory's proof lacks modularity in at least two ways. First, the proof contains multiple arguments, instead of breaking out sub-arguments as lemmas. For example, Ivory does not identify, as an inde-

[4]For an introduction to modularity and its significance, see (Avigad, 201?).

pendent result, the fact that $N, 2N, \ldots, (p-1)N$ can be represented as $m \cdot p + 1, m \cdot p + 2, \ldots, m \cdot p + (p-1)$ (in some order), nor does he separate the proof of this fact from the main body of his proof of Fermat's Little theorem. This means that the reader has to pay attention to the main argument of the proof, as well as the sub-argument, at the same time. This will increase her cognitive burden, as she has to identify the sub-argument herself and must consider whether a particular step is part of the sub-argument or the main argument. If the sub-argument was separately identified and proven, however, this work would be done for her and consequently her cognitive burden would be reduced.

The second way in which the proof lacks modularity is in the choice of representation of the sequence $N, 2N, \ldots, (p-1)N$. Recall that Ivory associates each member of this sequence with two further numbers, its quotient q and its remainder r when divided by p. Ivory tries to reduce the increased load this places on the reader's resources by introducing his '$m \cdot p$' notation. He is able to do this as he recognizes that the particular value of each quotient does not matter (it only matters that there is one), and his notation prevents the reader from having to remember a (potentially distinct) quotient for each element of the sequence. However, this approach does not completely reduce the additional information the reader has to handle, as she still has to carry the '$m \cdot p$' notation around, and also needs to perform operations involving it, such as expanding the product $(m \cdot p + 1) \times (m \cdot p + 2) \times (m \cdot p + 3) \ldots \times (m \cdot p + (p-1))$. In contrast, in a modern proof that utilizes congruence notation, the quotient is completely suppressed.

The lack of modularity in Ivory's proof means that the reader has to put in more effort to parse the proof and determine how the different parts of it depend on each other. This in turn means that she needs to apply more effort to recognize how the sequence $N, 2N, \ldots, (p-1)N$ contributes to the argument. Consequently, while the sequence is indeed contribution appropriate, the proof requires the reader to apply extra effort to recognize this.

There are similar difficulties when we consider the sequence from the point of view of introduction appropriateness. It is partially introduction appropriate because it connects to the context and the statement of the theorem in a direct manner: first, N appears $(p-1)$ times in the sequence, which is significant given that the result states $N^{p-1} - 1$ is evenly divisible by p. Thus it is possible to give at least a reasonable partial answer to the question

"Where does this step come from?" However, a similar connection to the multiplicands $1, 2, 3, \ldots, (p-1)$ is missing. Certainly there are $(p-1)$ of them, but this is a tenuous connection, as $(p-1)$ copies of N could be obtained in a variety of other ways.

As the sequence $N, 2N, 3N, \ldots, (p-1)N$ is only partially introduction appropriate, the reader can only partially recognize it as such. An alert reader should recognize the connection between the $(p-1)$ occurrences of N and the statement of the theorem with little difficulty, and thus should be expected to give at least a partial answer to the question "Where does this step come from?" However, given that the information relating to the choice of multiplicands $1, 2, \ldots, (p-1)$ is not readily available in her context, she should not be expected to recognize why this was selected. Consequently, she should not be expected to give a full answer to the question of where the step came from.

The Dirichlet-Dedekind style proof is better motivated than Ivory's, with respect to its minimal context. Recall that in Ivory's proof, I pointed to difficulties regarding the introduction of the sequence $N, 2N, \ldots, (p-1)N$. The corresponding step in the Dirichlet-Dedekind style proof is not subject to the same problems and helps the reader to answer similar questions that may arise. First, instead of introducing $\{a, 2a, \ldots, (p-1)a\}$, the proof begins by considering ax as x runs through $\{1, 2, \ldots, (p-1)\}$. Given the context, this is indeed contribution appropriate, and there is a satisfactory answer to the question of how it advances the argument. Indeed, it allows lemma (3.3.1) to be applied, and then the result follows by multiplying the terms of the sequence and applying the cancellation law.

Further, the way in which the Dirichlet-Dedekind style proof, as well as the background context, are structured helps the reader to recognize this and thus arrive at a satisfactory answer herself. First, the proof explicitly draws attention to the fact that $\{1, 2, \ldots, (p-1)\}$ and $\{a, 2a, \ldots, (p-1)a\}$ are reduced residue systems. This tells the reader what is important about them, and should also call to mind properties and results about such systems. Moreover, lemma (3.3.1) occupies a privileged position within the context, as it is explicitly identified as an important result. This should mean that it is close at hand when the reader considers reduced residue systems. Thus the proof and context work together to direct the reader's attention, which should help her to more easily grasp the argument.

Second, the Dirichlet-Dedekind style proof is more modular than Ivory's. Indeed, instead

of proving that $\{a, 2a, \ldots, (p-1)a\}$ is a permutation of $\{1, 2, \ldots, (p-1)\}$ directly, lemma (3.3.1) is invoked. Thus the reader can focus on one argument at a time, and does not have her cognitive load increased by having to follow multiple arguments simultaneously. Additionally, the use of congruence notation significantly streamlines the proof. In particular, it allows Ivory's '$m \cdot p$' notation to be dropped, thus reducing the amount of data the reader must carry around. This helps to reduce the reader's cognitive burden, and puts her in a favorable position to recognize how the step contributes to the argument. Consequently, the proof and context work together so that the reader should be able to satisfactorily answer how the step advances the argument. Thus the step is contribution appropriate, and recognizably so.

The step in which we consider ax as x runs through $\{1, 2, \ldots, (p-1)\}$ is also introduction appropriate. As with Ivory's proof, this introduces $(p-1)$ copies of a, which connects to the theorem to be proved. However, unlike Ivory's proof, the selection of $\{1, 2, \ldots, (p-1)\}$ can be connected to the current context. Indeed, it is an example of a reduced residue system, a concept which is included in the context, and any reduced residue system mod a prime p has $(p-1)$ elements, which also connects it to the statement to be proven. Further, lemma (3.3.1) is flagged as an important and useful result in the context, and this step allows that lemma to be applied, which is an additional strong connection to the context. These connections thus make it possible to give a satisfactory answer to the question of where the step comes from.

Additionally, the reader is in a good position to recognize these connections to the context and so should be able to answer the question of where the step comes from herself. Given the theorem to be proved, an alert reader should find it natural to look for $(p-1)$ copies of a. The reader should also know important results about reduced residue systems, in particular, that a reduced residue system mod p has precisely $(p-1)$ elements. This is enough to consider multiplying the elements of a reduced residue system by a to obtain $(p-1)$ copies of a. While the reader should recognize that any such system will work, $\{1, 2, \ldots, (p-1)\}$ is the simplest example, and thus a good one to start with. Additionally, as lemma (3.3.1) has been flagged as especially useful, it should be close at hand and thus the reader should recognize it can be applied. Consequently, the step is introduction appropriate, and the

reader should recognize it as such too.

Above I have suggested that Ivory's proof is not well motivated with respect to a minimal context, whereas the more modern Dirichlet-Dedekind style proof is better motivated, though with respect to a more sophisticated context. Now, I will consider the two proofs from a common context: the "union" of the two minimal contexts the proofs were evaluated against previously. The addition of an extra, less sophisticated, context seems unlikely to impact the degree to which the Dirichlet-Dedekind style proof is motivated. However, what about Ivory's proof? Might the additional mathematical tools in the new context, in particular the notion of reduced residue system and the associated important results, help? Consider again the very first step in which Ivory introduces the sequence $\{N, 2N, \ldots, (p-1)N\}$. Before I argued that this was only partially introduction appropriate, as the context did not account for the selection of the multiplicands $1, 2, \ldots, (p-1)$. However, in the augmented context, that information is available, and thus it is possible to give a satisfactory answer to the question of where it comes from. Consequently it seems reasonable to suggest that the step is now introduction appropriate. Nonetheless, it will not be as easy for the reader to recognize this, compared to the Dirichlet-Dedekind style proof. Indeed, Ivory's proof does not focus the reader's attention by identifying the relevant sequences as reduced residue systems like the Dirichlet-Dedekind proof. Further, in order to grasp the relevant connections between the proof and the updated context, the reader must translate Ivory's argument into the language of congruences, which creates an additional cognitive burden. Thus although it is now possible to give a satisfactory answer to the question of where it comes from, the reader should not be expected to find it as easily as she should with respect to the Dirichlet-Dedekind style proof.

Moreover, there is another impediment to the motivational power of Ivory's proof when considered against this new context: the extra resources render his '$m \cdot p$' notation extraneous and unnecessary. After all, the updated context has the resources to handle the calculations which are undertaken in Ivory's proof without introducing his new notation. Consequently, one might suggest that, considered from the new context, the proof violates an important convention: maintaining standardized notation. Violations of this convention can make it very difficult to control the resulting mathematics: just imagine if each proof introduced

its own idiosyncratic notation for common concepts. Certainly there may be a legitimate reason for breaking away from standard notation, perhaps to make it more suitable to a new context or in an attempt to generalize it, but otherwise it can be problematic. And it seems there is little reason for utilizing Ivory's notation, as opposed to congruence notation, when considering the proof of Fermat's Little Theorem. Indeed, as I highlighted above, Ivory's notation still requires the reader to carry around irrelevant information. Thus, the steps of Ivory's proof which utilize this notation may be deemed inappropriate. For while it is still possible to answer the questions of how they advance the argument and where they come from, these answers are not completely satisfactory, given that they deviate from the conventions in operation in the new context. Of course, Ivory can't be faulted for using this notation himself, as Gauss' notation had only been introduced a few years previously and was not standardized.

Conclusions

Pre-theoretically, Ivory's proof appeared to be lacking motivation as some of its steps provoked unanswerable questions. The Dirichlet-Dedekind proof, on the other hand, appeared more successful because corresponding questions about its steps could be given a satisfactory answer. These questions provide a useful way of thinking about the contribution and introduction appropriateness of a proof step, and whether it is recognizably appropriate. The important question from the point of view of contribution appropriateness is, as I highlighted above, "How does this step advance the argument?", while the crucial question for introduction appropriateness is "Where does this step come from?" Whether there is a satisfactory answer to these questions will depend on the context and the resources available within it, as was highlighted in the case study. If it is possible to give a satisfactory answer to the relevant question, then the step is contribution or introduction appropriate, respectively. However, just because it is *possible* to give a satisfactory answer to these questions, it does *not* mean that a reader *should be expected to* arrive at such an answer herself. If, however, the reader should be expected to obtain these answers, then the step is recognizably contribution appropriate, or recognizably introduction appropriate, respectively.

In terms of factors that can impact the motivational efficacy of a proof, the above case

study highlighted at least two: the extent to which a proof is modularized, and the context against which it is evaluated. As I discussed above, a modular proof helps the reader to manage information effectively, and reduces the cognitive burden that she must bear when parsing the steps in the proof. This means that she should have more cognitive resources to spend on other tasks, such as identifying connections between different parts of the proof and the context itself. Thus a modular proof should put the reader in an improved position to recognize the appropriateness of steps in the proof by helping her to obtain satisfactory answers to the questions of how the step advances the argument and where it comes from. However, as already emphasized, the context also plays a significant role in whether a proof is motivated or not. Moreover, there are four different features of the context that must be taken into consideration: the tools that it contains, the manner in which it is organized, the values which are in operation and the conventions that it establishes.

The resources that are available within the context can impact both whether a step is appropriate and whether it should be recognized as such by the reader. For example, with Ivory's proof, the minimal context it was considered against did not contain enough resources to fully anchor the selection of $\{N, 2N, \ldots, (p-1)N\}$, and it thus failed to be introduction appropriate. In the Dirichlet-Dedekind style proof, however the concept of a reduced residue system was available, which did serve to anchor the corresponding step, thus making it introduction appropriate. Moreover, the Dirichlet-Dedekind style proof leveraged this concept by explicitly indicating that $\{1, 2, \ldots, (p-1)\}$ and $\{a, 2a, \ldots, (p-1)a\}$ are reduced residue systems. This directed the reader's attention to their important properties, namely, those that they have in virtue of being such systems. This consequently helps the reader to manage information in the proof, and should make it easier for her to recognize the appropriateness of the proof steps.

The structure or organization of the context can also impact the degree to which a proof is motivated. A context that has internal structure, such as an indication of which resources are particularly useful or important, can help ensure that proofs are well motivated. For example, if there are tools in the context that are flagged as important or useful, then they should be more easily recognized by a reader when they are appealed to within a proof. The Dirichlet-Dedekind style proof made use of the structure of the context in just this way:

recall that lemma (3.3.1) was identified within the minimal context as being an important result, and was subsequently appealed to within the proof of Fermat's Little theorem. This technique helps the reader to recognize both the contribution the reduced residue systems make, as well as where they come from.

Additionally, the structure of the context can impact what steps are appropriate, not just which are recognized as appropriate. Indeed, steps that invoke tools identified within the context as important or useful will be strongly connected to the context, and this may help to ensure that they are appropriate. Indeed, utilizing such privileged tools may be one way to improve the quality of possible answers to the questions "How does this step advance the argument?" and "Where does it come from?" Of course, this is not the only factor to be taken into consideration, and can be overridden, for example, if certain values or goals are taken to be part of the context, such as obtaining a proof that restricts the use of certain techniques for purity considerations etc. Thus the current values or goals can also impact whether a step is appropriate with respect to a given context.

Finally, there are the conventions associated with a context. Breaking such conventions goes against the "rules" associated with the context and can thus render proof steps inappropriate, unless there is a compelling reason to break them. For example, congruence notation is now a standard way of representing calculations involving division when we do not care about the quotient, but only the remainder. Thus, when considered against a context that involves modular arithmetic, Ivory's proof breaks convention as he introduces his '$m \cdot p$' notation. Consequently, the steps in his proof which utilize this notation are, at least to some extent, inappropriate, as possible answers to the questions of how the steps advance the proof and where they come from fail to be completely satisfactory.

3.4 Wilson's Theorem

In modern terminology, Wilson's theorem states the following: if p is a prime then $(p-1)! \equiv -1 \mod p$. The statement of this theorem was first published by Edward Waring in 1770, who attributed it to John Wilson (Dickson, 2012, 62). The first proof was given by Joseph-

Louis Lagrange in the early 1770s and many other different proofs followed.[5] In this section I will discuss Lagrange's original proof, as well as a more modern presentation found in Dirichlet-Dedekind's *Vorlesungen*.

Before considering the proofs in detail, it will be useful to sketch the components involved in each proof:

Sketch of Core Argument

The key idea is to introduce a polynomial which has a particular form and whose constant coefficient is $(p-1)!$. Features of the polynomial are then exploited to calculate its constant coefficient. Lagrange does this directly via computation, while Dirichlet and Dedekind appeal to Fermat's Little theorem and other general results about polynomials.

3.4.1 Lagrange's 1773 Proof

Although some of the ideas in Lagrange's proof are subtle, it uses only elementary mathematics. Thus, to follow Lagrange's argument, the reader only need be familiar with elementary number theory, algebra and some combinatorics. More specifically, the reader needs to: perform simple algebraic manipulations, including manipulations on polynomials, perform simple combinatorial calculations, such as calculating binomial coefficients, be familiar with key properties of prime numbers, such as Euclid's lemma, and perform simple proofs by induction.

Lagrange's proof was published in 1773, before Gauss' congruence notation was available. His statement of Wilson's theorem thus looks different to the modern formulation, and is as follows:

> *If n is a prime number, then the number $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \ldots (n-1)+1$ will always be divisible by n;*
>
> that is to say that the continued product of numbers 1, 2, 3, ..., until $(n-1)$ inclusive, being increased by 1, will be divisible by n, or better, that if you divide that product by the prime number n, we have -1, or, what amounts to the same

[5] See (Dickson, 2012, 59–104) for a comprehensive survey.

thing, $n-1$ for the residue.[6] (Lagrange, 1773, 425)

Lagrange began his proof by introducing the polynomial $(x+1)(x+2)(x+3)(x+4)\dots(x+n-1)$. Expanding it, he obtained:

$$\begin{aligned}&(x+1)(x+2)(x+3)(x+4)\dots(x+n-1)\\&=x^{n-1}+A'x^{n-2}+A''x^{n-3}+A'''x^{n-4}+\dots+A^{(n-1)}\end{aligned}$$

where the coefficients are to be determined. To do so, he remarked that the above equation holds when x is replaced by $x+1$. Thus

$$\begin{aligned}&(x+2)(x+3)(x+4)(x+5)\dots(x+n)\\&=(x+1)^{n-1}+A'(x+1)^{n-2}+A''(x+1)^{n-3}+A'''(x+1)^{n-4}+\dots+A^{(n-1)}\end{aligned}$$

Multiplying this equation by $x+1$, and then comparing it to the first equation multiplied by $x+n$ yields

$$\begin{aligned}&(x+n)(x^{n-1}+A'x^{n-2}+A''x^{n-3}+A'''x^{n-4}+\dots+A^{(n-1)})\\&=(x+1)^n+A'(x+1)^{n-1}+A''(x+1)^{n-2}+A'''(x+1)^{n-3}+\dots+A^{(n-1)}(x+1)\end{aligned}$$

Expanding and collecting like terms gives the following:

$$\begin{aligned}&x^n+(n+A')x^{n-1}+(nA'+A'')x^{n-2}+(nA''+A''')x^{n-3}+\dots\\&=x^n+(n+A')x^{n-1}+\left[\frac{n(n-1)}{2}+(n-1)A'+A''\right]x^{n-2}\\&+\left[\frac{n(n-1)(n-2)}{2\cdot 3}+\frac{(n-1)(n-2)}{2}A'+(n-2)A''+A'''\right]x^{n-3}+\dots\end{aligned}$$

[6]The English translation is my own. The original French text is as follows: "Si n est un nombre premier quelconque, le nombre $1\cdot 2\cdot 3\cdot 4\cdot 5\cdot(n-1)+1$ sera toujours divisible par n; c'est-à-dire que le produit continuel des nombres 1, 2, 3, jusqu'à $n-1$ inclusivement, étant augmenté de l'unité, sera divisible par, n, ou bien, que si l'on divise ce même produit par le nombre premier n, on aura -1, ou, ce qui est la même chose, $n-1$ pour reste."

Next, Lagrange compared like terms to obtain the following equations:

$$\begin{aligned}
&n + A' = n + A' \\
&nA' + A'' = \frac{n(n-1)}{2} + (n-1)A' + A'' \\
&nA'' + A''' = \frac{n(n-1)(n-2)}{2 \cdot 3} + \frac{(n-1)(n-2)}{2}A' + (n-2)A'' + A''' \\
&\dots
\end{aligned}$$

From these, he derived the following relations:[7]

$$\begin{aligned}
A' &= \frac{n(n-1)}{2} \\
2A'' &= \frac{n(n-1)(n-2)}{2 \cdot 3} + \frac{(n-1)(n-2)}{2}A' \\
3A''' &= \frac{n(n-1)(n-2)(n-3)}{2 \cdot 3 \cdot 4} + \frac{(n-1)(n-2)(n-3)}{2 \cdot 3}A' + \frac{(n-2)(n-3)}{2}A'' \\
&\dots
\end{aligned} \tag{3.1}$$

Notice that the coefficients $A', A'', A''', \dots, A^{(n-1)}$ are integers. Further, notice that $A^{(n-1)}$ is $1 \cdot 2 \cdot 3 \cdot \ldots \cdot (n-1)$.

Next Lagrange established the following theorem:

Theorem 3.4.1. *If n is a prime, then $A', A'', A''', \dots, A^{(n-2)}$ are all divisible by n. Further, n divides $A^{(n-1)} + 1$.*

Proof. If n is prime, then n clearly divides each of $\frac{n(n-1)}{1 \cdot 2}$, $\frac{n(n-1)(n-2)}{1 \cdot 2 \cdot 3}$, $\dots$, apart from $\frac{n(n-1)(n-2)\dots 1}{1 \cdot 2 \cdot 3 \dots \cdot n}$ which is obviously 1. Using this fact, and the relations proved in (3.1), above, it follows inductively that $A', 2A'', 3A''', \dots, (n-2)A^{(n-2)}$ are all divisible by n. Thus, as n does not divide $1, 2, 3, \dots, (n-2)$, Lagrange concluded that n must divide each of $A', A'', A''', \dots, A^{(n-2)}$.

[7] For example, consider the first equation below, $A' = \frac{n(n-1)}{2}$. This is obtained by subtracting $A'' + (n-1)A'$ from both sides of the second equation above, $nA' + A'' = \frac{n(n-1)}{2} + (n-1)A' + A''$. Lagrange, however, did not provide any explanation of the calculations in his original exposition.

Next Lagrange considered $(n-1)A^{(n-1)}$. Using the relations in (3.1), he derived the following:

$$\begin{aligned}(n-1)A^{(n-1)} &= \frac{n(n-1)(n-2)\dots 1}{1\cdot 2\cdot 3\cdot \dots \cdot n} \\ &+ \frac{(n-1)(n-2)\dots 1}{1\cdot 2\cdot 3\cdot \dots \cdot (n-1)}A' + \frac{(n-2)(n-3)\dots 1}{1\cdot 2\cdot \dots \cdot (n-2)}A'' \\ &+ \dots \\ &= 1 + A' + A'' + A''' + \dots + A^{(n-2)}.\end{aligned}$$

Adding $A^{(n-1)}$ and subtracting $A' + A'' + A''' + \dots + A^{(n-2)}$ from both sides, he obtained:

$$A^{(n-1)} + 1 = nA^{(n-1)} - A' - A'' - A''' - \dots - A^{(n-2)}$$

Finally, as $A', A'', A''', \dots, A^{(n-2)}$ are all divisible by n, it follows that $A^{(n-1)} + 1$ is also divisible by n. □

As it was noted above that $A^{(n-1)} = 1\cdot 2\cdot 3\cdot \dots \cdot (n-1)$, Lagrange's proof of theorem (3.4.1) also establishes Wilson's theorem. □

However, Lagrange did not stop here. Rather, he used the same technique to obtain a proof of Fermat's Little Theorem. First, he noted that, in general, if x is an integer, then his previous calculations establish that $(x+1)(x+2)\dots(x+n-1) - x^{n-1} + 1$ is always divisible by n, so long as n is prime. Further, if x is an integer not divisible by n, then one of the following must be divisible by n: $x+1, x+2, \dots, x+n-1$. Thus the product $(x+1)(x+2)\dots(x+n-1)$ must also be divisible by n. Consequently, $x^{n-1} - 1$ must also be divisible by n, which is Fermat's Little Theorem. Lagrange thought his proofs were advantageous, precisely because they highlight "…the connection and mutual dependence between these two theorems" (Lagrange, 1773, 430)

3.4.2 Dirichlet's Proof

A similar proof of Wilson's theorem was included in Dirichlet-Dedekind's *Vorlesungen über Zahlentheorie*. They expressed Wilson's theorem as follows: "When p is a prime number,

one plus the product of the positive integers less than p is divisible by p. In symbols, $1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv -1 \mod p$"(Stillwell, 1999, 42). The proof utilizes similar ideas to those found in Lagrange's work, but it is different and, in particular, assumes the reader to have access to more advanced mathematical tools.

In particular, to follow the proof, the reader should be competent with: elementary number theory, algebra and modular arithmetic. Additionally, the context should explicitly include two important theorems: Fermat's Little theorem and the Polynomial Representation theorem. Dirichlet expressed the Polynomial Representation theorem as follows:

> *... if the nth degree congruence*
>
> $$f(x) \equiv 0 \mod p$$
>
> *whose modulus p is a prime, has n incongruent roots* $\alpha, \beta, \gamma, \ldots, \lambda$*, then its left hand side is of the form*
>
> $$(3)\ f(x) = a(x-\alpha)(x-\beta)(x-\gamma)\ldots(x-\lambda) + p\psi(x)$$
>
> *where a is the leading coefficient of* $f(x)$ *and* $\psi(x)$ *is a polynomial with integer coefficients* (Stillwell, 1999, 40–41).

This theorem occupies a privileged position in the background context, as Dirichlet-Dedekind explicitly stated that it is one of two theorems "... which are of the greatest importance in what follows" (Stillwell, 1999, 41).

I'll now present a summary of Dirichlet-Dedekind's proof (see (Stillwell, 1999, §27)). Recall that the aim is to prove that $(p-1)! \equiv -1 \mod p$. Dirichlet-Dedekind began by noting that, by Fermat's Little Theorem, each of $1, 2, 3, \ldots, (p-1)$ satisfy $x^{p-1} - 1 \equiv 0 \mod p$. Clearly $1, 2, 3, \ldots, (p-1)$ are all incongruent mod p, so by the Representation Theorem for polynomials:

$$x^{p-1} - 1 = (x-1)(x-2)(x-3)\ldots(x-p+1) + p\psi(x) \tag{3.2}$$

where $\psi(x)$ is a polynomial with integer coefficients.

They then noted that, if p is an odd prime, the constant coefficient of $(x-1)(x-2)(x-3)\ldots(x-p+1)$ is

$$(-1)^{p-1} \cdot 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1).$$

Next, Dirichlet-Dedekind expanded the polynomial on the right hand side of (3.2), and noted that coefficients of each power of x must be congruent mod p to the corresponding coefficient of the polynomial on the left hand side. This means, in particular, that the constant terms are congruent mod p.

This shows that $1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \equiv -1 \mod p$ for an odd prime p.

Moreover, the result clearly holds when $p = 2$ as $1 \equiv -1 \mod p$.

Thus Wilson's Theorem is proved. □

3.4.3 Discussion of the Proofs of Wilson's Theorem

Analysis

As with the discussion of the proofs of Fermat's Little theorem, I will first analyze Lagrange's proof and Dirichlet-Dedekind's proof with respect to distinct "minimal" contexts, before considering them from a common context. As before, by "minimal", I mean a context that at least provides the reader with enough mathematics to verify the correctness of each of the steps, but potentially does not go beyond this. For Lagrange's proof, the minimal context will consist of elementary number theory and algebra, including Euclid's lemma, techniques for manipulating algebraic expressions, e.g. expanding a polynomial and calculating its coefficients, and the technique of proof by induction. In addition, as it was important to Lagrange, I will take the context to contain the value of unifying Fermat's Little theorem and Wilson's theorem by establishing them via a common technique. For Dirichlet-Dedekind's proof, the context will be more sophisticated and include modular arithmetic, elementary

number theory and algebra. Thus it will contain e.g. the definition of congruence and basic techniques for manipulating simple congruences, as well as techniques for algebraic manipulations and simple arithmetical calculations. In addition, it should contain two important theorems: Fermat's Little theorem and the Polynomial Representation theorem, with the latter being flagged as having particular significance. Unlike the context associated with Lagrange's proof, this context will not include the value of unifying Fermat's Little theorem and Wilson's theorem by establishing them by a common technique. The common context will then be the "union" of these two minimal contexts.

Pre-theoretically, Lagrange's proof is not particularly well motivated when considered with respect to its minimal context, as the proof raises questions which a reader should not be expected to answer without difficulty. For example, after reading the proof, the reader will likely wonder exactly how the polynomial $(x+1)(x+2)(x+3)(x+4)\dots(x+n-1)$ advances the argument, as well as pondering where it came from. Additionally, at one point in his proof, Lagrange multiplies one equation by $x+1$ and another by $x+n$ before equating them—the reader may similarly question how these manipulations advance the proof and where they come from. However, Dirichlet-Dedekind's proof fares far better when considered with respect to its minimal context. Indeed, the proof and context work together to help the reader to answer questions about how the steps advance the argument and where they come from. Nonetheless, when both proofs are considered from a common context, neither fare well. As the proofs display varying degrees of motivational efficacy when considered with respect to these different contexts, at least pre-theoretically, I will analyze them in detail to more concretely identify the source of their differences.

In section (3.3.3), I noted that a lack of modularity negatively impacted the motivational efficacy of Ivory's proof. Lagrange's proof of Wilson's theorem exhibits a similar lack of modularity. First, while Lagrange did try to give the proof structure by identifying certain sub-results, this does not succeed in keeping information localized and thus his proof fails to be highly modular. For example, the coefficients $A', A'', \dots, A^{(n-1)}$ appear throughout the proof, even though the only coefficient that we are directly interested in is $A^{(n-1)}$. More precisely, theorem (3.4.1) tells us the remainders of all of the A^i when divided by n, instead of separating the result about the "middle coefficients", $A', A'', \dots, A^{(n-2)}$, which are all

divisible by n, from Wilson's theorem itself. Second, Lagrange did not make strategic use of abbreviations to hide information when it is not directly relevant: he kept all information on full display. For example, he did not introduce notation to abbreviate the polynomial $(x+1)(x+2)(x+3)(x+4)\dots(x+n-1)$ or its expansion: he worked with the full expressions in his proof. And, as before, this lack of modularity makes it difficult for the reader to parse the proof and to determine how each of the parts work together.

In particular, the lack of modularity will make it harder for the reader to identify the contribution that the polynomial makes to the argument. A satisfactory answer is available given the context: the coefficients of this polynomial enjoy a (recursive) relationship, which allows for their remainders upon division by n to be easily calculated. More precisely, the (recursive) relationship is used to establish that the "middle coefficients", $A', A'', \dots, A^{(n-2)}$, are all divisible by n. This fact and the recursive relationship are then used together to demonstrate that $A^{(n-1)}+1$ is divisible by n, which is Wilson's theorem. However, isolating the structure of the argument is not easy for the reader because there is a lot of information that she must assess and keep track of, and because the information is not particularly localized. Thus, while the first step of Lagrange's proof is contribution appropriate, it fails to be recognizably so.

Similarly, the lack of modularity makes it more difficult for the reader to determine where the multiplicands $(x+1)$ and $(x+n)$ come from. Recall that after expanding the polynomial $(x+1)(x+2)(x+3)(x+4)\dots(x+n-1)$ to obtain $x^{n-1}+A'x^{n-2}+A''x^{n-3}+A'''x^{n-4}+\dots+A^{(n-1)}$, Lagrange instructed the reader to substitute $x+1$ in place of x to obtain $(x+1)^{n-1}+A'(x+1)^{n-2}+A''(x+1)^{n-3}+A'''(x+1)^{n-4}+\dots+A^{(n-1)}$. He next instructed the reader to multiply the first expansion by $(x+n)$ and the second by $(x+1)$ and then equate them. While the reader can verify that these two expressions are equal, she may wonder how he found $(x+1)$ and $(x+n)$, as it is not obvious by just looking at the polynomial expansions. However, an answer is available, though Lagrange's proof obscures it, and I will describe it when presenting a more modular proof below. Consequently, Lagrange's algebraic manipulations in this step are introduction appropriate, but are not recognizably so.

While a lack of modularity negatively impacts Lagrange's proof, it can be made much more modular by making a few small changes. Indeed, in 1859, Julius Toeplitz (Toeplitz,

1859) presented such a proof.[8] First, Toeplitz abbreviated the polynomial $(x+1)(x+2)(x+3)(x+4)\dots(x+n-1)$ as $f(x)$.[9] Like Lagrange, Toeplitz expanded this to obtain:

$$f(x) = x^{n-1} + A'x^{n-2} + A''x^{n-3} + A'''x^{n-4} + \dots + A^{(n-1)}.$$

He noted immediately that the constant coefficient of this polynomial is of interest, since $f(0) = (n-1)! = A^{n-1}$. To determine the value of the other coefficients (considered mod n), Toeplitz substituted $x+1$ for x in $f(x)$, like Lagrange. This yields

$$f(x+1) = (x+2)(x+3)\dots(x+n) = \frac{(x+n)f(x)}{(x+1)},$$

and hence

$$(x+1)f(x+1) = (x+n)f(x).$$

Toeplitz then proceeded just as Lagrange had done, expanding the polynomials and comparing coefficients to determine that $A', A'', \dots, A^{(n-2)}$ are all divisible by n.

Having established this, however, Toeplitz continued in a different manner from Lagrange. In particular instead of appealing directly to the equations in (3.1), Toeplitz derived Wilson's theorem from the following lemma[10]:

Lemma 3.4.2. *for any integer x,*

$$(x+1)(x+2)(x+3)(x+4)\dots(x+n-1) - x^{n-1} - (n-1)!$$

must be divisible by n.

This lemma holds as the "middle coefficients", $A', A'', \dots, A^{(n-2)}$, are all divisible by n, and the constant coefficient $A^{(n-1)}$ is $(n-1)!$.

[8] In his proof, Toeplitz used a different polynomial than Lagrange: $(x-1)(x-2)\dots(x-n+1)$. However, I will adapt Toeplitz's argument for Lagrange's original polynomial, for ease of comparison. Additionally, Toeplitz made use of congruence notation, which was not available to Lagrange, and this further increases the modularity of his proof.

[9] Toeplitz's actual abbreviation was fx but I am using modern function notation.

[10] However, Toeplitz did not identify this result explicitly as a lemma.

Wilson's theorem then follows almost immediately from lemma (3.4.2). Indeed, as it holds for any x, it holds for $x = 1$. Thus $(2 \cdot 3 \cdot 4 \ldots \cdot n) - 1 - (n-1)!$ must be divisible by n. But as $2 \cdot 3 \cdot 4 \ldots \cdot n$ is clearly divisible by n, this means that $(n-1)! + 1$ must be divisible by n and Wilson's theorem is established.

Toeplitz's proof thus keeps information more localized than Lagrange's. More specifically, the coefficients $A', A'', \ldots, A^{(n-2)}$ do not feature throughout the entire proof, but only in establishing lemma (3.4.2). Toeplitz's proof also hides information when it is not relevant to the reader by making strategic use of notation. For example, Toeplitz named the polynomial and referred to this abbreviation when the fuller expression was not needed. This increased modularity helps the reader to better grasp how the steps advance the argument and where they come from.

More precisely, Toeplitz's proof helps the reader to identify the contribution that the polynomial makes to the argument, for a number of reasons. First, Toeplitz's strategic use of abbreviations means that the reader has less data that she must keep track of, which reduces the burden on her cognitive resources and means she can focus on identifying how the pieces of the proof work together. Second, the Toeplitz style proof is more highly structured. Indeed, it includes an additional lemma: lemma (3.4.2). The polynomial $f(x)$ reappears in this lemma and is easily recognizable. Further, Wilson's theorem follows straightforwardly from lemma (3.4.2). The reader should thus be able to recognize that the polynomial is important as it is used to establish lemma (3.4.2), from which Wilson's theorem can be derived without difficulty. In addition, as already mentioned above, information in Toeplitz's proof is more localized, as the middle coefficients are separated from the coefficient of primary interest, $A^{(n-1)}$. This makes it easier for the reader to determine the role that the middle coefficients themselves play in the proof, which in turn will help her to appreciate the role of the polynomial.

The increased modularity of Toeplitz's proof also makes it clear to the reader where the multiplicands $(x + 1)$ and $(x + n)$ come from. Indeed, by focusing on the polynomials, instead of their expansions, and by making strategic use of abbreviations, Toeplitz directs

the reader's attention to the relevant information:

$$f(x+1) = (x+2)(x+3)\dots(x+n) = \frac{\mathbf{(x+n)}f(x)}{\mathbf{(x+1)}}.$$

This makes the relationship much clearer than Lagrange's version, which included irrelevant information:

$$\begin{aligned}&(x+n)(x^{n-1} + A'x^{n-2} + A''x^{n-3} + A'''x^{n-4} + \dots + A^{(n-1)})\\ &= (x+1)^n + A'(x+1)^{n-1} + A''(x+1)^{n-2} + A'''(x+1)^{n-3} + \dots + A^{(n-1)}(x+1)\end{aligned}$$

However, although increasing the modularity of Lagrange's proof increases its motivational value, it does little to help the reader answer another pressing question: "Where does the polynomial $(x+1)(x+2)\dots(x+n-1)$ come from?" The reader can indeed see, as Lagrange pointed out later in the proof, that the constant coefficient of the polynomial is $(n-1)!$, but this does not provide insight into the choice of factors or the degree of the polynomial, for example. Thus the proof still seems to be somewhat motivationally deficient. An answer is available within the minimal context, however. Indeed, if x is an integer, then $(x+1)(x+2)\dots(x+n-1)$ is a product of $n-1$ consecutive integers starting at $x+1$, just as $(n-1)!$ is a product of $n-1$ consecutive integers starting at 1.[11] The reader should not be expected to notice the relevance of this right away, however. Indeed although there is a close connection between integers and polynomials, to notice the relevant commonality in this case requires the reader to translate between domains. Unless she is presented with a reason to do this, for example, a strategy in the context that is being applied requires it, the proof should prompt her. Otherwise, she may not notice it. Once it is drawn attention to, however, the reader can strongly connect the polynomial to $(n-1)!$ and should be able to grasp where the factors and degree come from.

In summary, then, Lagrange's proof is not well motivated with respect to its minimal context, not because the steps fail to be appropriate, but because a reader should not be expected to recognize their appropriateness. Indeed, while answers to questions like "How

[11] This is highlighted in connection with the discovery of Lagrange's theorem for polynomials by Friedberg in his book *An Adventurer's Guide to Number Theory* (Friedberg, 1995, 163).

does this step advance the argument?"; "Where does this step come from?" are available, they are obscured from the reader.

Dirichlet-Dedekind's proof, however, is much better motivated when considered with respect to its minimal context. Indeed, the structure of the proof and the context should help the reader to answer questions about how the steps contribute to the argument and where they come from. First of all, Dirichlet-Dedekind's proof is highly modular. More precisely, information in the proof is localized and, in some cases, entirely removed. For example, instead of performing calculations to show directly that $x^{p-1} - 1 = (x-1)(x-2)(x-3)\dots(x-p+1) + p\psi(x)$, Dirichlet-Dedekind refer to a more general result within the context: the Polynomial Representation theorem. Work is required to read and digest the proof of this theorem, but providing it separately from the proof of Wilson's theorem prevents the reader from having to consider two proofs simultaneously, which in turn frees up her cognitive resources.

However, it is not just the modular structure of Dirichlet-Dedekind's proof that is responsible for its motivational efficacy. In addition, the proof and the context work together to highlight relevant connections, which helps the reader to grasp where the proof steps come from. Consider, for example, the introduction of the polynomial $x^{(p-1)} - 1$. Dirichlet-Dedekind introduced this after noting that each of the multiplicands 1, 2, ..., $(p-1)$ in $(p-1)!$ all have a common property: they all are subject to Fermat's Little theorem. Attempts at expressing this in a general way lead naturally to the polynomial $x^{p-1} - 1$. Further, the context highlights the Polynomial Representation theorem as a particularly important result. Because of this, and because the reader can see that the conditions for application of the theorem are met, she should recognize that applying it is a natural next step, and thus recognize where this step comes from.

Having considered Lagrange's proof and Dirichlet-Dedekind's with respect to their minimal contexts, I'll now consider them with respect to a common context. The common context consists of all of the resources and structure associated with the two minimal contexts. In addition, as the minimal context for Lagrange's proof has the associated value of unifying Fermat's Little theorem and Wilson's theorem, this value should be added to the common context. Considered with respect to this context, Lagrange's proof will, pre-theoretically,

remain unmotivated. Indeed, the difficulties it faced when considered against the minimal context will remain. Similarly, Dirichlet-Dedekind's proof will, pre-theoretically, appear unmotivated, though for a different reason: it does not respect the value of unifying Fermat's Little theorem and Wilson's theorem. Indeed, the very first step of Dirichlet-Dedekind's proof appeals to Fermat's Little theorem and so the two are not obtained via a common technique. This means that there are no fully *satisfactory* answers to the questions of how the step advances the argument and where it comes from for this context. Indeed, while the step advances the argument and connects strongly to the context, it does not do so in a way that respects the value of unifying Fermat's Little theorem and Wilson's theorem. Thus this step is neither contribution nor introduction appropriate.

Conclusions

The analysis of proofs of Wilson's theorem supports the claim, made in section (3.3.3), that motivational efficacy is closely related to whether there are satisfactory answers to questions such as "How does this step advance the argument?"; "Where does this step come from?", and whether the reader should be expected to uncover these answers. Indeed, I suggested that Lagrange's proof, considered with respect to a minimal context, is unmotivated, and that while answers to those two questions were available, a reader shouldn't be expected to find them. In contrast, Dirichlet-Dedekind's proof, considered against its minimal context, is well motivated, and a closer inspection revealed that the proof and its context provide answers to questions concerning the contribution and reasons for introduction of each of the steps. Further, they helped the reader to uncover these answers. Finally, I suggested that both proofs fail to be well motivated when considered against the union of the minimal contexts. For Lagrange's proof, answers are still difficult for the reader to uncover, and for Dirichlet-Dedekind's proof, satisfactory answers are no longer available.

Additionally, the degree to which a proof is modular, and certain features of the context against which it is evaluated, again impacted the motivational efficacy of the analyzed proofs. In particular, Toeplitz's and Dirichlet-Dedekind's modular proofs were seen to be better motivated than Lagrange's less modular proof. Further, the structure of the context, as well as the appended values, impacted the motivational efficacy of Dirichlet-Dedekind's

proof. Indeed, as before, elevating certain resources in the context to a privileged status strengthened the connection of steps appealing to them to the context, as well as helping the reader to better recognize such connections. This helped to make proof steps that refer to them introduction appropriate, and recognizably so. However, the values associated with the common context negatively impacted the motivational efficacy of Dirichlet-Dedekind's proof by rendering previously satisfactory answers about the contribution a step makes, or reasons for its introduction, unsatisfactory. I suggested this theoretically in section (3.3.3) but Dirichlet-Dedekind's proof, considered against the common context, provides a real example of this phenomenon.

Chapter 4

A Theory of Motivated Proofs

4.1 Preliminary Remarks

Having analyzed three elementary case studies in chapter 3, I will now develop a theory of motivated proofs. As part of the theory, I will first elaborate on the notions of *proof*, *context*, (recognizable) *correctness* and (recognizable) *appropriateness* of steps, before proposing criteria that a proof should meet to be considered motivated with respect to a particular context. Additionally, I will explain the primary benefits of motivated proofs, and argue that these benefits justify the claim that obtaining such proofs should be a mathematical goal. However, the work I undertake in this chapter is just a preliminary investigation: these notions require much further clarification and development.

4.2 Ingredients

4.2.1 Proof

As the case studies from chapter 3 have illustrated, the way in which a proof is organized and the notation that it uses can have a significant impact on its (pre-theoretical) motivational efficacy. In what follows, I will thus take such features to be included in my notion of proof. Admittedly this stretches the common-sense understanding of the term, since on this conception even minor organizational or notational changes would cause one proof to be

transformed into a different one. If this is considered to be highly problematic, "proof" can be replaced with "proof implementation" in what follows and the theory of motivated proofs I develop becomes a theory a motivated proof implementations.

4.2.2 Mathematical Context

As I highlighted in chapter 3, a proof is (or fails to be) motivated with respect to a mathematical context. Thus, before proposing a definition of motivated proofs, I will first describe the notion of a context in more detail. Recall that, in chapter 3, I likened a context to a "mathematical toolbox", containing certain tools and being arranged in a particular way. Thus the context was seen to possess not only *resources*, but a *structure* as well. In the analysis of Fermat's Little theorem in section (3.3.3) and Wilson's theorem in section (3.4.3), I suggested that, in addition, the context contains associated *conventions* and *values*, which can also affect the motivational efficacy of a proof.

The resources possessed by a mathematical context include *definitions*, for example of particular concepts, e.g. reduced residue systems mod m, or of particular mathematical objects or entities, e.g. π as the ratio of a circle's circumference to its diameter. Relatedly, the context can contain *instantiations* of these definitions, e.g. $\{1, 2, 3, 4\}$, a reduced residue system mod 5. The resources may also include *mathematical results*, for instance the Polynomial Representation theorem and, additionally, particular *proofs* of the theorem. Furthermore, the resources can contain an arsenal of mathematical *techniques*, in other words, standard approaches that can be used again and again to establish results. As examples, consider the technique of proof by induction for a number theory context, or double counting for a combinatorial one.[1] Finally, the contextual resources may include *heuristics*, which are guidelines for solving a particular kind of problem. For example, a student may be told that if she needs to prove that, given a particular integer k, for any positive integer n, $f(n)$ is divisible by k, she should first try a proof by mathematical induction. In what follows, it will be helpful to focus on the *written representation* of these resources. I will say more about this below.

[1]Double counting involves establishing a combinatorial identity by showing that each side of the proposed identity is a different way of counting the same set. For examples, see e.g. (Benjamin and Quinn, 2003).

As highlighted in the case studies, the resources in the context will often have a particular structure or organization. One way in which they may be structured is by ranking them. For example, certain definitions, examples, theorems, proofs, techniques or heuristics might be singled out as being particularly important or useful, while the others less so (though perhaps with further distinctions among the less important resources, too). Another way in which they may be organized is by being grouped together in a particular manner. For example, resources that are often used together may be placed in one group. A further way in which they may be organized is in terms of what they are "about", with all (and only) the resources about a particular topic collected together.

It may be difficult to visualize how the structure and organization of the context is to be understood. However, as I suggested above, focusing on a written representation of the contextual resources can be helpful. Understood in such a way, the structure of the context can be viewed as similar to a textbook. Thus the grouping together of certain resources can be represented by placing those resources within the same chapter or section of the text. Alternatively, if the resources are in different chapters or sections, an explicit note concerning their relation or association could be made. Similarly, an explicit note can serve to highlight the privileged, important resources against the less important ones.

Conventions are the next component in the mathematical context. The conventions establish standards that practitioners of the context should follow and expect others to follow regarding, for example, the application of certain contextual resources. As with the resources, it may be useful to conceive of the conventions as being explicitly written down. It might be thought that these do not have to be made explicit and can simply be inferred from examining the resources and structure of the context, but this is not the case. Indeed, the resources will likely under-determine the conventions. For example, in section (3.3.3), I suggested that, from a modern context, Ivory's proof fails to be well motivated, in part because there is a violation of modern conventions: Ivory's proof is framed in terms of divisibility instead of congruences. However, the modern context contains resources about divisibility *and* about congruences and so the resources in this case do not allow us to infer the conventions in operation.

Values are the final ingredient in the mathematical context. They are somewhat different

from the other components in that they can be selective, in the sense of only applying to particular proofs. Ideally, the values should specify which proofs (or kinds of proofs) they apply to and be accompanied by precise criteria for satisfaction. For example, instead of expressing a preference for 'simplicity', a suitable value should, say, express a preference for proofs that do not rely upon a certain 'heavy duty' lemma or other resource. More generally, the criteria for satisfaction of a particular value should be understood as modifying the rest of the context. In particular, they may restrict the resources that can be appealed to, or alter the structure or conventions that are in place.

As was highlighted by the case studies discussed in chapter 3, each of the four components of the context can affect the motivational efficacy of a proof considered against it.

4.2.3 (Recognizable) Correctness

In discussing the case studies in chapter 3, I focused primarily on the *appropriateness* of the proof steps and, further, whether their appropriateness should be recognizable to the reader. However, it is important to note that the correctness of the steps, and the recognizability of their correctness, are also crucial if a proof is to be well motivated. Indeed, if a proof step fails to be correct, the "proof" is not a proof at all, and thus cannot be well motivated. Further, if the reader should not be expected to recognize the correctness of the proof steps, the argument will fail to appear as a proof and thus again it will not be well motivated.

Correctness, as I am understanding it, is context relative. In particular, the resources utilized in any given step must come from the current context;[2] if more sophisticated ones are used, then the step fails to be correct with respect to that context, though it may be correct with respect to an augmented one. As an illustration, consider intuitionist vs. classical logic. A proof step that is obtained from a prior line by double negation elimination will not be correct with respect to an intuitionistic context, but it will when considered against a classical one.

Recognizable correctness goes further than requiring the step to follow legitimately from the previous lines and the context. For a step to be recognizably correct, a reader with access

[2]A step that breaks conventions or values would not, on my account, be incorrect, but rather inappropriate.

to the context should be expected to verify for herself that it was obtained legitimately. While this may seem trivial, poor information management in the proof itself and in the context can make it difficult. Just imagine, for example, that to obtain a given step in a proof, a particular obscure result is applied. However, the proof does not reference the result itself, it simply applies it. Further, suppose that, while the result is included within the context, it is buried within one of the less important sections, so that it is difficult to recall without being prompted. Under such circumstances, the reader should not be expected to recognize the correctness of the proof step—it will likely take considerable effort to verify that it was legitimately obtained.

Finally, I should note that recognizable correctness is a matter of degree. The more difficult it is for a reader to verify that a step is legitimately obtained given the context, the less she should be expected to do so, and thus the less recognizably correct the step becomes. Features that can improve, or diminish, recognizable correctness are broadly similar to those that can impact recognizable appropriateness, and will be discussed below.

4.2.4 (Recognizable) Appropriateness

As discussed in chapter 3, there are (at least) two distinct kinds of appropriateness: contribution and introduction appropriateness. While these were discussed informally in section (3.2.2), the analysis in sections (3.3) and (3.4) suggested a more concrete manner of understanding them in terms of questions. Recall that a step is said to be contribution appropriate, relative to a given context, if it is possible to satisfactorily answer the question "How does this step advance the argument?" within that context. A step is said to be introduction appropriate, relative to a given context, if it is possible to satisfactorily answer the question "Where does this step in the argument come from?" within that context.[3] Notice that both kinds of appropriateness depend not only on the context, but also on the proof itself.

Although I will be leaving the notion of *satisfactory answer* mostly undefined, there are

[3]There are complications with the notions of contribution and introduction appropriateness that should be further explored. For example, sometimes the only available answer to the question "How does the step advance the argument?" and "Where does the step come from?" may be truly minimal ones, such as "It just works" or "It's just available". Presumably these answers will not generally be satisfactory, but perhaps there are some circumstances under which they are so.

a few clarificatory remarks that I would like to make. First, any potential answer must only appeal to resources available within the context, and it must adhere to the conventions and values, unless it provides compelling reasons to break them. Further, a potential answer should be plausible, given the context. For instance, considering the question "Where does X come from?", an answer of "Y", where X and Y are not connected within the context, would fail to be plausible. Additionally, satisfactory answers should be as complete as is practical, so that they address each component in the proof step. For instance, an answer which spells out where part of a particular proof step comes from, but provides very little information about the rest of the step, is somewhat satisfactory, but an answer that addresses all of the components would be more so. A further feature that can increase the quality of an answer is how strongly it connects a step to the context. In particular, answers that, for example, appeal to privileged resources arguably produce a stronger connection than those which appeal to more obscure ones. Finally, it may be helpful to think of a satisfactory answer as one a reader of the proof should accept, if it was given to her.

As Pólya noted and as I have illustrated further in chapter 3, it is not enough that the steps in a proof be appropriate for the proof to be well motivated; they must be recognized as such too. Recall that, in section (3.3.3) I suggested that a step is recognizably contribution or introduction appropriate with respect to a given context if there are satisfactory answers to the questions "How does this step advance the argument?" and "Where does this step in the argument come from?" respectively, and further, that the reader should be expected to uncover such answers herself. Thus, recognizable appropriateness also comes in degrees.

One important feature of a proof that can impact recognizable appropriateness is its degree of modularity. As I highlighted in sections (3.3.3) and (3.4.3), highly modular proofs introduce strategic abbreviations and localize information in self-contained modules, which can help to reduce the cognitive burden on the reader. Such proofs thus free up her resources for use elsewhere, such as in attempting to answer questions like "How does this step advance the argument?" and "Where does this step in the argument come from?".

A related feature is the degree to which a proof is broken down into different parts. Notice that this is weaker than modularity, as modularity requires that information is localized, and a proof can be divided into parts without ensuring this. For example, Lagrange's proof of

Wilson's theorem was decomposed into some (high level) parts, but information, in particular the polynomial coefficients, featured throughout the entire proof. Decomposing a proof into separate parts in this manner can impact the recognizable appropriateness of proof steps in a similar manner to modularity. In particular, by telling the reader how to break up the proof, it allows her to focus on one part at a time, instead of requiring her to figure out how to divide up the proof, which requires further cognitive resources. Further, a proof that is broken down into smaller parts can be particularly helpful with respect to recognizable contribution appropriateness. Indeed, such a proof will allow the reader to more easily identify which part of the proof the current step pertains to and this should then put her in an improved position to determine its role in more detail. However, as we saw with Lagrange's proof, the benefits of decomposing a proof can be far weaker than modularizing it. Indeed, the steps in Lagrange's proof were far less recognizably appropriate compared to the steps in Dirichlet-Dedekind's much more modular proof.

A final feature of the proof that can impact the recognizable appropriateness of its steps is the quality and number of annotations that the proof author provides. By an annotation I mean a note about a particular step in the proof, which can be a brief description of its purpose or why it was selected, or simply an indication that the reader needs to pay close attention to the step. As an example of the latter kind of annotation, consider Bourbaki's "dangerous bend" sign, or Knuth's variant,  . Of course, too many such annotations, or annotations in misleading places, will hinder, rather than help, the reader.

In addition, the components of the context can have a large impact on the recognizable appropriateness of the proof steps. As mentioned above, the conventions and values can impact whether a step is appropriate or not, and if a step fails to be appropriate it also fails to be recognizably appropriate. The available resources can similarly impact the appropriateness of proof steps, but they can also affect their recognizable appropriateness more directly. Indeed, the available resources can influence the complexity of an answer. As Dedekind wrote "...the greatest and most fruitful advances in mathematics and other sciences have invariably been made by the creation and introduction of new concepts, rendered necessary by the *frequent recurrence of complex phenomena which could be controlled by the old notions only with difficulty*" (Dedekind, 2008, 16, emphasis added). And the more

complex a satisfactory answer is, the less we should expect a reader to uncover it on her own.

The structure of a context can also impact recognizable appropriateness by making the resources accessible, or obscure and difficult to reach. For example, resources that are privileged, in the sense of being highlighted as important, will be readily recalled by the reader, but those that are buried within a technical section and hardly used will be much harder for the reader to recall. Thus an answer that relies on privileged resources will be easier for a reader to uncover than one which utilizes more obscure resources. Similarly, grouping resources together or separating them can impact recognizable appropriateness. For example, suppose that a satisfactory answer to the question of where a particular step S in a proof P comes from relies on a particular resource R. Further, assume that in context C, R is grouped together with Q, a resource that appears in step S, and that in context C', R is not grouped with Q. Under these circumstances, the answer should be more easy for the reader to uncover in context C than in C'. Thus step S of P is more recognizably appropriate in context C than in context C'.

4.3 A Definition of "Motivated Proofs"

For a proof to be well motivated with respect to a given context, the steps should all be correct, contribution appropriate, introduction appropriate and further their correctness and appropriateness should be recognized by the reader. Assuming that recognizable correctness implies correctness and recognizable appropriateness implies appropriateness, the definition can be stated more concisely as follows:

Motivated Proof [4] A proof P of theorem T is well motivated with respect to a particular

[4]Sieg suggests that there are two separate senses in which a proof can be well motivated. The first is an internal, mathematical sense of motivation. The second is an audience-focused, cognitive sense of motivation. My definition runs both of these senses together by requiring that the proof steps be correct and appropriate and further that they be recognized as such. In future work, it may be fruitful to keep the mathematical and cognitive aspects more distinct. This could be achieved, Sieg proposes, by making the definition of a motivated proof relative to a context and a reader separately, as this might help facilitate interdisciplinary work. Indeed, he suggests that it may be possible to utilize interactive theorem provers to determine whether a proof is well motivated with respect to a given context in a purely mathematical sense, and to use experiments to separately investigate whether it would be motivated to a reader in a cognitive, psychological sense.

context C if and only if each step S of P is:

1. recognizably correct with respect to C.

2. recognizably contribution appropriate with respect to C.

3. recognizably introduction appropriate with respect to C.

As recognizable appropriateness is a matter of degree, whether a proof is motivated with respect to a given context is also a matter of degree.

There are, however, some subtle issues that must be addressed. First, let me tackle a potential objection. Suppose that we have a proof P of theorem T, which is well motivated with respect to context C. Now suppose that we remove some steps from the end of P to obtain a "proof" P' (see figure 4.1). As the steps in P' are just a subset of the steps in P, it might be thought that all of the steps in P' are recognizably correct and recognizably appropriate. If this were true, then we might conclude that, according to my definition, P' is a well motivated proof of T, which is not at all desirable.

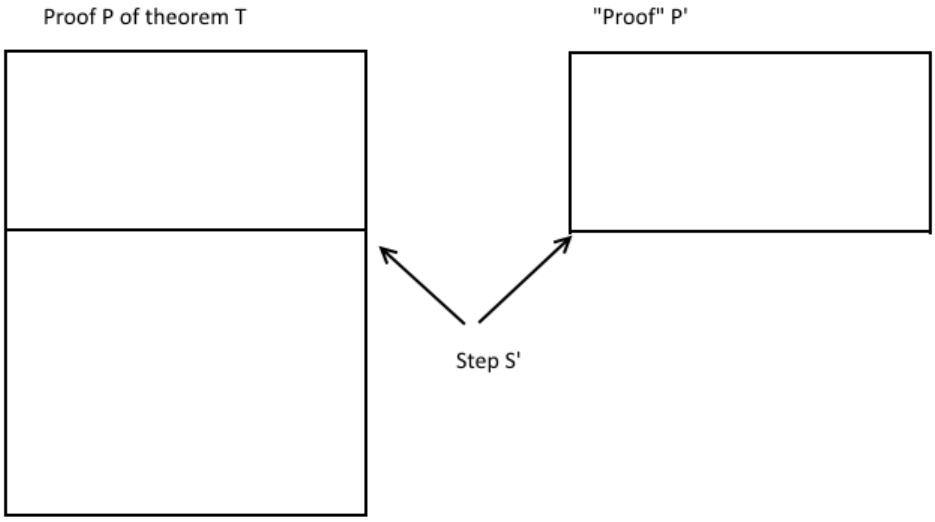

Figure 4.1: Removing steps from a motivated proof P.

However, even though the steps in P' are a subset of the steps in P, this does not mean that they are all recognizably appropriate. Indeed, as I mentioned above, whether a step is (recognizably) appropriate depends both on the context and the rest of the proof in which it is a part. As P and P' are not the same proof, it is possible for a step S to be recognizably appropriate in P but fail to be so in P', and this is just what happens in this situation.

More precisely, suppose that S' is the last step in P'. For S' to be contribution appropriate in P', there must be a satisfactory answer to the question "How does S' advance the proof P' of theorem T?" within the context. However, there is no satisfactory answer to this question. Indeed, the step S' does not advance the proof P' of theorem T, as P' terminates at that step and does not establish T. As the question has no satisfactory answer, step S' fails to be introduction appropriate in P' and thus P' is not a motivated proof of theorem T.

However, there are further complications that must be considered. More precisely, in section (4.2.4) I suggested understanding (recognizable) appropriateness in terms of questions such as "How does this step advance the argument?" and "Where does this step in the argument come from?" However, this is ambiguous because an argument or proof can be made up of several arguments or subproofs. For example, suppose that a proof P of theorem T is comprised of proofs $P_1, \ldots, P_n$ of lemmas $L_1, \ldots, L_n$ (see figure 4.2). Then if we have a step S_i that occurs in proof P_j of lemma L_j, there are in fact two proofs to consider: P_j and the main proof P of which P_j is a part.

In such a situation, the question "How does step S_i advance the argument?" can be decomposed into two questions: "How does step S_i advance the argument P_j in establishing L_j?" and "How does L_j advance the argument P in establishing T?" Similarly, the question "Where does the step S_i in the argument come from?" can be decomposed into the questions: "Where does step S_i come from in the argument P_j?" and "Where does L_j come from in the argument P?" It is reasonable to think that both versions of such questions matter for the motivational efficacy of a proof like P which is made up of various lemmas.

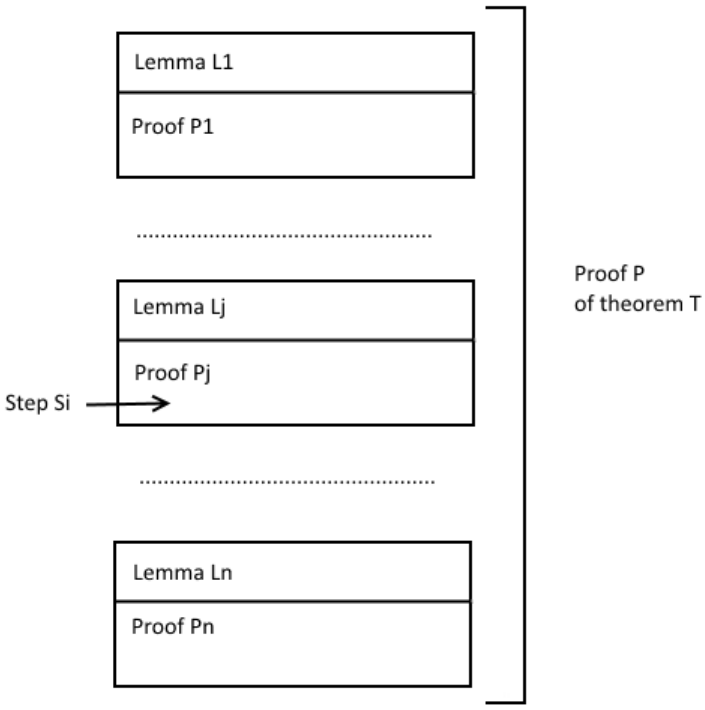

Figure 4.2: A compound proof P made up of subproofs $P_1, \ldots, P_n$ of lemmas $L_1, \ldots, L_n$.

This suggests that, in such cases, the lemmas $L_1, \ldots, L_n$ themselves can be viewed as steps in the main proof P. Thus we can say that proof P is well motivated with respect to the context C if and only if:

1. Each lemma L_j is:

   (a) recognizably correct[5]

   (b) recognizably contribution appropriate (wrt P and C)

   (c) recognizably introduction appropriate (wrt P and C)

and

2. Each step S_i in the proof P_j of L_j is:

[5]This reduces to each of the steps of L_j being recognizably correct.

(a) recognizably correct

(b) recognizably contribution appropriate (wrt P_j and C)

(c) recognizably introduction appropriate (wrt P_j and C)

4.4 Increasing Motivation

4.4.1 Preliminary Remarks

As highlighted above, motivational efficacy depends on both the proof under consideration and the context. Thus we can denote the motivational efficacy of a proof P with respect to a context C as $m(P, C)$. In discussing ways in which to improve the motivational efficacy of a proof, I will be considering changes that can be made to the proof P, resulting in a new proof P', as well as changes that can be made to the context, resulting in a new context C', that can help ensure $m(P', C') > m(P, C)$. However, this raises some important but subtle issues.

First, there is the question of what changes to the proof P are permissible. Indeed, if P' is obtained by radical enough changes we may no longer wish to say that we are "improving the motivational efficacy of P", but are instead starting anew. Second, there is the question of what changes to the original context C are permissible. This, in particular, is a crucial question. Indeed, if the context can be altered in any way we like, given any unmotivated proof we could presumably engineer an artificial context against which it is very well motivated. However, appeal to such an artificial context is problematic for at least two reasons. First, changes to a context will affect more than just one proof, and a context developed artificially for the express purpose of motivating one particular proof may well have an adverse affect on the motivational efficacy of other proofs considered against it. Second, allowing unrestricted changes to the context could make it prohibitively difficult for a reader with access to the old context to gain access to the new one. Yet if we are aiming to improve the motivational efficacy of a proof, we should want a reader with access to the original context to be able to transition to the new one so that she can reap the benefits of the better motivated proof.

I will not consider these issues in any more detail here, but they are important and need to be further developed.

4.4.2 Techniques for Improving Motivational Efficacy

The first question to consider when attempting to improve the motivational efficacy of a proof is whether it is deficient because one or more steps fail to be correct or appropriate with respect to the context. If the problem does lie with the correctness or appropriateness of the steps (instead of the recognizable correctness or appropriateness), then changes to the context or substantial reformulations of the proof may be the best course of action. For example, in section (3.3.3), I argued that one of the first steps in Ivory's proof of Fermat's Little theorem failed to be introduction appropriate because the context was not rich enough to anchor the selection of a particular sequence. Augmenting the context, and reformulating the proof could overcome this problem, however. Indeed, the first step in Dirichlet-Dedekind's proof of Fermat's Little theorem was introduction appropriate (and recognizably so), and the enhanced context, which was leveraged by the proof, was responsible.

Alternatively, a step may fail to be appropriate because attempts to articulate its role or where it comes from violate conventions or values in operation in the context. In some cases, there may be a reason for the transgression, which may suggest a reformulation of the context. However, in other cases, such as Ivory's proof of Fermat's Little theorem considered against a more modern context (see section (3.3.3)), there is no good reason and it is the proof that should be reformulated.

If it is not the correctness or appropriateness of the proof steps, but rather their recognizable correctness or appropriateness that is at issue, then there are further amelioratory actions that can be taken. If the proof is quite complex or if it is dealing with a large amount of information, it may be helpful to first try to break the proof up into parts or modularize it. In terms of decomposing the proof into parts, it may be helpful to provide the reader with an outline of the argument before filling in the details with the complete proof. Working through a simpler example or two, as seen in section (3.2), may be beneficial for similar reasons. Additionally, the proof editor should check that auxiliary results that are established within the proof are separately identified, so that when the proof reader is

working through the proof she can easily determine the goal of the current reasoning. Increasing the proof's modularity will take further work. To try to make a proof more highly modular, the proof editor could examine the notation used to see if it would be helpful to introduce abbreviations, though it is not always straightforward to determine the "right" level of detail required for a proof. Additionally, the editor could examine the proof and try to further localize information within it, which may take take the form of decomposing the proof into a series of sub-proofs of lemmas.

However, breaking a proof up into parts or modularizing a proof raises an important question: should the sub-proofs be added to the context or still be considered part of the main proof? Certainly, if the sub-proof is a result that is only (expected to be) relevant to the main proof then there is little reason to consider it separate and attempt to add it to the context. However, if the sub-proof is of a result that generalizes and is (expected to be) useful and relevant in other circumstances, then perhaps a case can be made for considering it to be independent of the main proof and adding it to the context.

If the proof has been broken into parts or is already highly modular, yet still faces difficulties regarding recognizable correctness or appropriateness, the proof editor may try to address the "problematic steps" more directly. First, the proof editor may be able to help the reader grasp where the problematic step comes from and the role that it plays by showing her how it fixes up a different, unsuccessful proof attempt. However, for this to be helpful, the reader should be better able to grasp where the steps in the unsuccessful attempt come from and the role that they were supposed to play. By showing the reader why this simpler approach fails and thinking about what might be needed to make it work, the reader should come to better grasp the role that the problematic step plays. Additionally, she should now be in a better position to see where the step comes from: the simpler approach, which would be better motivated if it were successful, fails and while trying to fix it, the more problematic step suggests itself. Indeed, as Pólya remarked "In some cases a plausible story of the discovery supplies an attractive motivation" (Pólya, 1949, 686). The motivational material that Pólya added to his proof of Carleman's inequality was of exactly this form.

Additionally, the proof editor could add an annotation to focus the reader's attention on the problematic step, such as making use of a "dangerous bend" sign. Perhaps more

satisfactorily, the editor may be able to give a brief note describing the role the troublesome step plays or indicating where it comes from. Indeed, the introduction of the polynomial in Lagrange's proof could have been made far more recognizably introduction appropriate if a small note had been added indicating that it shared a common form with $(p-1)!$. Another approach the editor could take would be to justify the step via heuristic reasoning. Indeed, motivational material 1 and 2 from section (3.2) provide examples of this.

4.5 Benefits of Motivated Proofs

Motivated proofs have a number of benefits, both theoretical and practical. Such benefits have as their source the fact that a motivated proof provides the reader with more information than an unmotivated one. Indeed, an unmotivated proof will leave the reader without answers to questions about the correctness or appropriateness of some of the steps in the argument, whereas a motivated proof will enable the reader to discover the answers to such questions.

On the theoretical side, this helps motivated proofs to promote understanding[6] in a number of ways. First, the additional information directly helps the reader to understand how the proof steps work together to obtain the result. Less directly, this additional information can help the reader to, for example, deepen her understanding of the contextual resources. For instance, a motivated proof can help the reader to better grasp the range of applicability of certain resources by showing her how they apply in a new situation. Of course, an unmotivated proof can also show the reader that a contextual resource can be used in a new way, but a motivated proof provides a reader with more, helping her not just to see *that* it can be used but potentially helping her to see *how* and *why* it can be used. Finally, a motivated proof can help boost understanding of the theorem itself. Indeed, if a reader knows how each step contributes to the argument and where it comes from, she should be in an improved position to grasp why certain conditions are included in the statement of the theorem, or whether they can be loosened and so on.

On the more practical side, the additional information motivated proofs provide can

[6] I do not intend to develop a theory of mathematical understanding here and am speaking pre-theoretically.

help the reader to become a better prover. For while my account of motivated proofs has focused on the perspective of a proof *reader*, such a reader can, as she tries to expand her mathematical knowledge beyond that which she has read, also become a *prover* herself.[7] When attempting to prove her own results, she will perhaps consider making similar steps to those she has seen employed in other proofs. In doing so, she should compare her current (mathematical) situation to previous ones, noting similarities and differences between them. However, a reader who has been exposed to well motivated proofs will have access to more relevant information for making and comparing analogies than a reader who has seen poorly motivated proofs. Indeed, suppose that A and B are both trying to obtain a proof of a particular theorem, though A has previously seen only motivated proofs, while B has seen only poorly motivated proofs. Then A will have access to information concerning the contributions that the steps in those proofs make and where they come from, which B lacks. Thus A will have more relevant information against which to compare her current situation with previous ones compared to B. This should put her in a better position to judge when a step or technique that has been used before could be applied successfully (albeit potentially modified) than B. Consequently motivated proofs help a reader to reuse mathematical ideas and thus assists her in transforming into a producer, and not just a consumer, of mathematical results.

The benefits of motivated proofs, promoting understanding and reusability, thus help to make mathematics more accessible. However, this does not mean that motivated proofs should only be of concern in strictly pedagogical contexts. Indeed, making mathematics more accessible and stimulating further mathematical development are closely linked. As a concrete example consider Hilbert's famous *Zahlbericht*, a report on the state of algebraic number theory in 1895. Hilbert's aim in this work was "... to describe the results of the theory of algebraic number fields, with their proofs, in a logical development and from a unified point of view and *so to contribute towards bringing nearer the time when the achievements of our great classical authors of number theory become the property of all mathematicians*" (Hilbert, 1998, ix, emphasis added). However, as Franz Lemmermeyer and Norbert Schap-

[7]Future discussion of motivated proofs should more deeply explore the distinction between reader and prover.

pacher point out, he intended his unified theory to "...then also point the way to further research" (Hilbert, 1998, xxv). Thus accessibility and further mathematical development went hand-in-hand for Hilbert.

Motivated proofs thus have a number of important benefits, which help promote the development of the discipline. Because of this, mathematicians are justified in taking it to be a mathematical goal to obtain such proofs.

4.6 Concluding Remarks

Although my account of motivated proofs focuses on cognitive and pragmatic issues, it is not "merely" cognitive or pragmatic. Indeed, cognitive and pragmatic features are of philosophical significance, as they can be related to questions about the fundamental nature of our mathematical entities. More specifically, when developing new (or refining existing) mathematics we have to decide what the mathematical entities in the domain are like, and this is usually reflected in our presentation. On the other hand, presentational issues can also shape our conception of mathematical entities. More precisely, while our mathematical presentations must be clear and well defined, we also require that they can cope with complex reasoning in an effective way. Sometimes, however, our presentations are shown to be ineffective, and this prompts a change in the way the entities themselves are understood. In the next chapter, I present a case study that highlights exactly this phenomenon.

Ultimately, certain cognitive and pragmatic issues are not so easily separable from other, more traditionally philosophical, topics about the nature of mathematics.

Chapter 5

A More Complex Case Study

5.1 Introduction

Having outlined my theory of motivated proofs in chapter 4, I will now demonstrate how it can be applied to a more complex case study from number theory: Dirichlet's theorem for primes in an arithmetic progression. In analyzing the case study, I aim to be sensitive to the historical context, and highlight the difficulties that can be encountered when attempting to better motivate a proof. In this case study, I will draw extensively on work I completed in my master's thesis (Morris, 2011), and subsequent joint papers with Avigad (Avigad and Morris, 2014; Avigad and Morris).

Dirichlet's theorem on primes in an arithmetic progression can be stated as follows:

Theorem 5.1.1 (Dirichlet's theorem)**.** *Any arithmetic progression whose first term a and common difference k are coprime contains infinitely many primes.*

By way of illustration, consider the arithmetic progression with first term 3 and common difference 4. Then the first 10 terms, with the primes indicated in bold, are:

$$\mathbf{3}, \mathbf{7}, \mathbf{11}, 15, \mathbf{19}, \mathbf{23}, 27, \mathbf{31}, 35, 39 \ldots$$

Dirichlet's theorem then tells us that this sequence, if continued indefinitely, will contain infinitely many primes.

To see why we need the condition that the first term and common difference are coprime, consider the arithmetic progression with first term 2 and common difference 4. Then the first 10 terms, with the primes indicated in bold, are:

$$\mathbf{2}, 6, 10, 14, 18, 22, 26, 30, 34, 38, \ldots$$

Notice that each term is of the form $2(1 + 2k)$, and so the progression only contains one prime.

Dirichlet offered the first proof of theorem (5.1.1) in 1837 (Dirichlet, 1837a). His work was ground-breaking and marked the birth of a new area of mathematics: analytic number theory. However, as we will see, there are a number of features of his original work that impact its motivational efficacy. Thus, before presenting Dirichlet's own proof, I will provide a modern version. The strategy used in the modern presentation, however, is very close to Dirichlet's own.

In order to understand the modern proof of Dirichlet's theorem, it is helpful to remember Euler's proof of the infinitude of the primes. I will thus first give a sketch of a modern proof of this result, following the presentation in Everest and Ward (Everest and Ward, 2006, 13–16). As we will see later, there are strong connections between this proof and the proof of Dirichlet's theorem. Indeed, Dirichlet noted that his proof of theorem (5.1.1) was inspired by Euler (Dirichlet, 1837b, 309–310).

5.1.1 Infinitude of the Primes

Euler established the infinitude of the primes by proving the following theorem:

Theorem 5.1.2. *$\sum_{p\ prime} \frac{1}{p}$ diverges.*

Clearly, this tells us that there must be infinitely many primes, as otherwise the sequence could not diverge.[1]

To prove theorem (5.1.2), we need the zeta function, which is defined for a real variable s as follows:

[1] In fact, it tells us more. As we know that $\sum_n \frac{1}{n^2}$ is convergent, we thus know that there are, in a sense, "more" primes than square numbers.

Definition Let $s \in \mathbb{R}$. Then $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$.

For the moment, we can ignore questions of convergence and just think of $\zeta(s)$ as a formal power series. However, $\zeta(s)$ converges when $s > 1$.

Crucial for the proof is the fact that the zeta function can also be represented as a product:

Theorem 5.1.3 (Euler Product formula)**.** *For any* $s > 1$, $\sum_{n=1}^{\infty} n^{-s} = \prod_p (1 - p^{-s})^{-1}$.

As Davenport puts it "this identity is an analytic equivalent for the proposition that every natural number can be factorized into prime powers in one and only one way" (Davenport, 2013, 2). However, I omit the full proof here.[2] Given the Euler Product formula, we can derive theorem (5.1.2) as follows. We begin by taking logarithms of both sides of the Euler Product formula. Recalling that $\log(ab) = \log(a) + \log(b)$ and $\log(a^b) = b \log(a)$, we thus obtain:

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

Next, recall the Taylor series expansion for $\log(1 - x)$:

$$\log(1 - x) = -\sum_{n=1}^{\infty} \frac{x^n}{n} \text{ when } |x| < 1.$$

If $s > 1$, then $|p^{-s}| < 1$ and we can thus make use of the Taylor series expansion for $\log(1 - p^{-s})$. Applying this to the above formula yields:

$$\log\left(\sum_{n=1}^{\infty} \frac{1}{n^s}\right) = \sum_p \sum_{n=1}^{\infty} \frac{1}{np^{sn}}.$$

As the series involved have suitably nice properties, we are able to change the order of summation:

$$\log\left(\sum_{n=1}^{\infty} \frac{1}{n^s}\right) = \sum_p \frac{1}{p^s} + \sum_p \sum_{n=2}^{\infty} \frac{1}{np^{sn}}.$$

[2] See (Everest and Ward, 2006, 14–15) for details.

Moreover, the right-most sum is bounded by a constant. Thus we have

$$\log\left(\sum_{n=1}^{\infty}\frac{1}{n^s}\right)=\sum_{p}\frac{1}{p^s}+\mathcal{O}(1).$$

Further, notice that $\log\left(\sum_{n=1}^{\infty}\frac{1}{n^s}\right)$ tends to infinity as s tends to 1 from above. This means that the sum on the right hand side, $\sum_p \frac{1}{p^s}$, must also tend to infinity as s tends to 1 from above. This tells us that $\sum_p \frac{1}{p}$ diverges and thus theorem (5.1.2) is proven. □

5.2 A Modern Proof of Dirichlet's Theorem

The proof of Dirichlet's theorem is, as mentioned above, closely related to Euler's proof that there are infinitely many primes. Recall that Dirichlet's theorem states that for any positive coprime integers a and k, the arithmetic progression $a, a+k, a+2k, \ldots, a+nk, \ldots$ contains infinitely many primes. Equivalently, we can state the result in the following form: there are infinitely many primes of the form $p = a + nk$, i.e. there are infinitely many primes $p \equiv a \mod k$. Thus, we can try to adapt Euler's strategy and establish Dirichlet's theorem by demonstrating the following result:

Theorem 5.2.1. $\sum_{p\equiv a \mod k}\frac{1}{p}$ *diverges*

To adapt Euler's strategy, we'll need a more general version of the Euler-Product Formula. Fortunately, this formula does generalize for series of the form $\sum_n^{\infty}\frac{f(n)}{n^s}$ provided $f(n)$ is *completely multiplicative*:

Definition A function $f:\mathbb{N}\to\mathbb{C}$ is completely multiplicative if and only if $f(1)=1$ and for all $m,n\in\mathbb{N}$, $f(mn)=f(m)f(n)$.

The generalized Euler-Product Formula is then as follows:[3]

Theorem 5.2.2 (General Euler-Product Formula)**.** *If $f(n)$ is a completely multiplicative function and $\sum_n^{\infty}\frac{f(n)}{n^s}$ is absolutely convergent, then*

$$\sum_{n}^{\infty}\frac{f(n)}{n^s}=\prod_{p}\left(1-\frac{f(p)}{p^s}\right)^{-1}.$$

[3]For more details and a proof see e.g. (Everest and Ward, 2006, 170).

As Dirichlet's theorem focuses on a subset of the primes, namely those which are congruent to $a \bmod k$, we need to be able to pick them out from the rest. The indicator function $e_{a,k}$ for the set of natural numbers congruent to $a \bmod k$ provides a natural way to do this. It is defined as follows:

$$e_{a,k}(n) = \begin{cases} 1 & \text{if } n \equiv a \mod k \\ 0 & \text{if } n \not\equiv a \mod k \end{cases}$$

We might then try to mimic Euler's argument in the following way:

Danger! Incorrect reasoning ahead!

$$\sum_{n=1}^{\infty} \frac{e_{a,k}(n)}{n^s} = \prod_p \left(1 - \frac{e_{a,k}(p)}{p^s}\right)^{-1}.$$

Thus, taking logarithms of both sides:

$$\begin{aligned} \log\left(\sum_{n=1}^{\infty} \frac{e_{a,k}(n)}{n^s}\right) &= -\sum_p \log\left(1 - \frac{e_{a,k}(p)}{p^s}\right) \\ &= \sum_p \sum_{n=1}^{\infty} \frac{e_{a,k}(p)^n}{np^{ns}} \\ &= \sum_p \frac{e_{a,k}(p)}{p^s} + \sum_p \sum_{n=2}^{\infty} \frac{e_{a,k}(p)^n}{np^{ns}} \\ &= \sum_{p \equiv a \mod k} \frac{1}{p^s} + \mathcal{O}(1). \end{aligned}$$

If we can show that $\log\left(\sum_{n=1}^{\infty} \frac{e_{a,k}(n)}{n^s}\right)$ diverges as $s \to 1$ then we will have shown that $\sum_{p \equiv a \mod k} \frac{1}{p}$ must also diverge, as required.

While the above reasoning seems promising, it is actually incorrect and fails at the very first line. Indeed, the indicator function $e_{a,k}$ is *not* completely multiplicative. For example, if $a = 3$ and $k = 4$ then $e_{3,4}(7) = e_{3,4}(11) = 1$, since $7 \equiv 3 \mod 4$ and $11 \equiv 3 \mod 4$. However, $e_{3,4}(77) = 0$ since $77 \equiv 1 \mod 4$. Thus

$$e_{3,4}(77) = e_{3,4}(7 \times 11) \neq e_{3,4}(7) \times e_{3,4}(11),$$

and so $e_{3,4}$ fails to be completely multiplicative.[4]

However, we can try to fix things by decomposing the indicator function $e_{a,k}$ into functions which are completely multiplicative. Finite Fourier analysis provides us with a way to do exactly this. In what follows, I will sketch an outline of this theory that is based on the excellent presentation in Stein and Shakarchi (Stein and Shakarchi, 2011, chapter 7).

Finite Fourier analysis takes place on a finite abelian group G, i.e. a group with a finite number of elements and a commutative group operation. The goal is to take a function $f : G \to \mathbb{C}$ and express it as a sum of more "well behaved" functions. For our purposes, the functions are more "well behaved" in the sense that they are completely multiplicative. More precisely, the functions are group homomorphisms called characters:

Definition Let G be a finite abelian group. Then a character e on G is a group homomorphism from G to $S^1 = \{z \in \mathbb{C} : |z| = 1\}$.[5] In other words, for any $a, b \in G$

$$e(a \cdot b) = e(a)e(b).$$

The set of characters on a finite abelian group G is denoted by $\widehat{G}$ and it inherits the group structure from G. In particular, it is easy to check that $\widehat{G}$ is an abelian group under the following group operation:

$$\text{For any } a \in G,\ (e_1 \cdot e_2)(a) = e_1(a)e_2(a).$$

The group identity element is provided by the trivial character, e_0, which takes the value 1 for all $a \in G$. Further G is isomorphic to $\widehat{G}$, and so there are exactly as many characters on G as there are elements of G.

As a concrete example of characters on a finite abelian group, consider the set of congruence classes mod 10 that are coprime to 10: $\{1, 3, 7, 9\}$. This forms an abelian group under multiplication and has four characters defined on it, as illustrated below:

[4] In fact, this shows that $e_{3,4}$ fails to be multiplicative. A function $f : \mathbb{N} \to \mathbb{C}$ is said to be multiplicative if and only if $f(1) = 1$ and for any coprime a, b, $f(ab) = f(a)f(b)$.

[5] S^1 is a group under multiplication.

	e_0	e_1	e_2	e_3
1	1	1	1	1
3	1	i	-1	$-i$
7	1	$-i$	-1	i
9	1	-1	1	-1

As seen above, the characters are complex valued functions on a finite abelian group G. More generally, however, the set of complex valued functions on G forms a vector space with dimension $|G|$. This means that they are closed under (pointwise) addition and scalar multiplication (with the scalars taken from $\mathbb{C}$). Further, we can equip the vector space with additional structure by defining a Hermitian inner product as follows:[6]

$$(f, g) := \frac{1}{|G|} \sum_{a \in G} f(a)\overline{g(a)}.$$

If V is a vector space, then a Hermitian inner product is a function $(,) : V \times V \to \mathbb{C}$ satisfying the following properties:

1. For any $f, g, h \in V$, $(f + g, h) = (f, h) + (g, h)$.
2. For any $f, g \in V$ and any $\alpha \in \mathbb{C}$, $(\alpha f, g) = \alpha(f, g)$.
3. For any $f, g \in V$ $(f, g) = \overline{(g, f)}$.
4. For any $f \in V$, $(f, f) \geq 0$ with equality holding only if $f = 0$.

Properties 1 and 2, above, will be particularly important later on.

With this set up we can then state the following crucial result:[7]

Theorem 5.2.3. *Let G be a finite abelian group and V the vector space of complex valued functions over G, equipped with the Hermitian inner product (f, g). Then the characters on G form an orthonormal basis for V.*

[6] We can think of a Hermitian inner product as a generalization of the familiar dot product from Euclidean space.

[7] See (Stein and Shakarchi, 2011, 232–234) for a proof of this theorem.

To say that the characters on G form a basis for V means that any function $f \in V$ can be represented as a linear combination of the characters. In other words,

$$f = \sum_{e \in \widehat{G}} \alpha_e e,$$

where $\alpha_e \in \mathbb{C}$. To say that the characters form an orthonormal basis means, in addition, that they satisfy the following conditions:

1. For any $e \in \widehat{G}$, $(e, e) = 1$.
2. If $e, e' \in \widehat{G}$ and $e \neq e'$ then $(e, e') = 0$.

With this background, we can now move on to the central result in finite Fourier analysis: that a function $f \in V$ is equal to its Fourier series expansion. To state this precisely, we first need to define the notions of Fourier coefficient and Fourier series.

Definition Let G be a finite abelian group and V the vector space of complex valued functions on G. Further, let $f \in V$ and $e \in \widehat{G}$. Then the Fourier coefficient of f with respect to e is defined as

$$\widehat{f}(e) := (f, e) = \frac{1}{|G|} \sum_{a \in G} f(a)\overline{e(a)}.$$

Definition Let G, V and f be as above. Then the Fourier series of f is defined to be

$$\sum_{e \in \widehat{G}} \widehat{f}(e)e.$$

Now we can prove the core result, mentioned above:

Theorem 5.2.4. *Let G be a finite abelian group, and V the vector space of complex valued functions on G, equipped with the inner product (f, g) defined above. Then if $f \in V$, f is equal to its Fourier series expansion:*

$$f = \sum_{e \in \widehat{G}} \widehat{f}(e)e.$$

Proof. As the characters of G form an orthonormal basis for V, we can write f as a linear combination of characters as follows:

$$f = \sum_{e \in \widehat{G}} \alpha_e e.$$

To show that f is equal to its Fourier expansion, $\sum_{e \in \widehat{G}} \widehat{f}(e)e$, I will show that for any $e' \in \widehat{G}$, $(f, e') = \alpha_{e'}$.

$$\begin{aligned}(f, e') &= (\sum_{e \in \widehat{G}} \alpha_e e, e') \\ &= \sum_{e \in \widehat{G}} \alpha_e (e, e') \text{ by properties 1 and 2 of Hermitian inner products} \\ &= \alpha_{e'} \text{ by orthogonality of characters}\end{aligned}$$

Thus

$$f = \sum_{e \in \widehat{G}} \alpha_e e = \sum_{e \in \widehat{G}} (f, e)e = \sum_{e \in \widehat{G}} \widehat{f}(e)e.$$

□

Now let us return to the matter of representing the function $e_{a,k}$ as a linear combination of completely multiplicative functions. First, it will be helpful to consider another indicator function which is defined on the set of congruence classes coprime to k. Let us define this function as follows:

$$d_{a,k}(\bar{n}) = \begin{cases} 1 & \text{if } \bar{n} = \bar{a} \\ 0 & \text{if } \bar{n} \neq \bar{a} \end{cases}$$

The set of congruence classes that are coprime to k form a finite abelian group under multiplication, denoted by $\mathbb{Z}^\star(k)$. Thus $d_{a,k}$ is a member of the vector space of complex valued functions on $\mathbb{Z}^\star(k)$. Hence, by the above results from Fourier analysis, $d_{a,k}$ is equal

to its Fourier series expansion:

$$d_{a,k}(\bar{n}) = \sum_{e \in \mathbb{Z}^\star(k)} \widehat{d_{a,k}}(e) e(\bar{n}),$$

where

$$\begin{aligned}
\widehat{d_{a,k}}(e) &= (d_{a,k}, e) \\
&= \frac{1}{|\mathbb{Z}^\star(k)|} \sum_{m \in \mathbb{Z}^\star(k)} d_{a,k}(\bar{m}) \overline{e(\bar{m})} \\
&= \frac{1}{|\mathbb{Z}^\star(k)|} \overline{e(\bar{a})} \text{ by definition of } d_{a,k}.
\end{aligned}$$

Thus

$$d_{a,k}(\bar{n}) = \frac{1}{|\mathbb{Z}^\star(k)|} \sum_{e \in \mathbb{Z}^\star(k)} \overline{e(\bar{a})} e(\bar{n}).$$

We can now define $e_{a,k}$ in terms of $d_{a,k}$:

$$e_{a,k}(n) = \begin{cases} d_{a,k}(\bar{n}) & \text{if } n \text{ is coprime to } k \\ 0 & \text{if } n \text{ is not coprime to } k \end{cases}$$

Similarly, we can "lift" the characters e on $\mathbb{Z}^\star(k)$ to all integers by defining their corresponding Dirichlet character.

Definition Let e be a character on $\mathbb{Z}^\star(k)$. Then the corresponding Dirichlet character is defined as:

$$\chi_e(n) = \begin{cases} e(\bar{n}) & \text{if } n \text{ is coprime to } k \\ 0 & \text{if } n \text{ is not coprime to } k \end{cases}$$

We call the Dirichlet character that corresponds to the trivial character, e_0, the trivial Dirichlet character and denote it as χ_0.

It is easy to check that for each e, the corresponding function χ_e is completely multiplicative. In what follows, I will simply refer to a Dirichlet character χ_e as χ.

Putting this all together now allows us to represent $e_{a,k}$ as a linear combination of completely multiplicative functions:

Theorem 5.2.5 (Representation of $e_{a,k}$)**.** *For any n,*

$$e_{a,k}(n) = \frac{1}{|\mathbb{Z}^\star(k)|} \sum_{\chi} \overline{\chi(a)}\chi(n).$$

Now we are in a better position to try to adapt Euler's strategy. The presentation here follows that of Everest and Ward (Everest and Ward, 2006, chapter 10), though I will skip over some subtle issues relating to the use of complex logarithms and convergence properties of the series involved.

The first step is to introduce functions more general than the zeta function, called L-functions:

Definition Let s be a complex variable and χ a Dirichlet character. Then the L-function associated with χ is

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

Note that L-functions converge so long as $\mathbb{R}(s) > 1$.

As Dirichlet characters are completely multiplicative, each L-function has a corresponding Euler product:

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{p} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}.$$

Assuming $\mathbb{R}(s) > 1$, we can take the logarithm of each side of the Euler-Product expansion, just like in Euler's proof.

$$\begin{aligned}
\log L(s,\chi) &= \sum_{p} -\log\left(1 - \frac{\chi(p)}{p^s}\right) \\
&= \sum_{p} \sum_{m=1}^{\infty} \frac{1}{m} \frac{\chi(p^m)}{p^{sm}} \\
&= \sum_{p} \frac{\chi(p)}{p^s} + \sum_{p} \sum_{m=2}^{\infty} \frac{\chi(p^m)}{mp^{sm}} \\
&= \sum_{p} \frac{\chi(p)}{p^s} + \mathcal{O}(1)
\end{aligned}$$

Now recall, from theorem (5.2.5), that for any prime p

$$|\mathbb{Z}^\star(k)|e_{a,k}(p) = \sum_\chi \overline{\chi(a)}\chi(p).$$

Thus, if we multiply both sides of the equation

$$\log L(s,\chi) = \sum_p \frac{\chi(p)}{p^s} + \mathcal{O}(1)$$

by $\overline{\chi(a)}$ and sum over all Dirichlet characters χ, we get:

$$\begin{aligned}
\sum_\chi \overline{\chi(a)} \log L(s,\chi) &= \sum_\chi \overline{\chi(a)} \sum_p \frac{\chi(p)}{p^s} + \mathcal{O}(1) \\
&= \sum_p \frac{1}{p^s} \sum_\chi \overline{\chi(a)}\chi(p) + \mathcal{O}(1) \\
&= |\mathbb{Z}^\star(k)| \sum_p \frac{e_{a,k}(p)}{p^s} + \mathcal{O}(1) \\
&= |\mathbb{Z}^\star(k)| \sum_{p \equiv a \mod k} \frac{1}{p^s} + \mathcal{O}(1)
\end{aligned}$$

This is promising! To complete the proof of Dirichlet's theorem, we need two more results:

Theorem 5.2.6. *$L(s,\chi_0)$ has a simple pole at $s = 1$.*

Theorem 5.2.7. *If $\chi \neq \chi_0$ then $L(s,\chi)$ has a finite non-zero limit as $s \to 1$.*

Theorem (5.2.6) and part of theorem (5.2.7) are straightforward to prove. However, establishing theorem (5.2.7) when the character in question takes only real values requires serious and difficult mathematical work. While I omit the proofs here, the reader should not underestimate the importance and depth of these theorems.

Assuming theorems (5.2.6) and (5.2.7), we can conclude that the left hand side of

$$\sum_\chi \overline{\chi(a)} \log L(s,\chi) = |\mathbb{Z}^\star(k)| \sum_{p \equiv a \mod k} \frac{1}{p^s} + \mathcal{O}(1)$$

Infinitude of the primes

1. $\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \prod_{p} \left(1 - p^{-s}\right)^{-1}$
2. $\log \zeta(s) = \sum_{p} \sum_{n=1}^{\infty} \frac{1}{np^{sn}}$
3. $\log \zeta(s) = \sum_{p} p^{-s} + \mathcal{O}(1)$
4. $\log \zeta(s) \to \infty$ as $s \to 1$

$\therefore \sum_{p} p^{-1}$ diverges.

Dirichlet's theorem

1′. $L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{p} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$

2′. $\log L(s,\chi) = \sum_{p} \sum_{n=1}^{\infty} \frac{\chi(p^n)}{np^{sn}}$

3′. $\log L(s,\chi) = \sum_{p} \frac{\chi(p)}{p^s} + \mathcal{O}(1)$

4′. $\sum_{\chi} \overline{\chi(a)} \log L(s,\chi) = \sum_{p} \frac{1}{p^s} \sum_{\chi} \overline{\chi(a)}\chi(p) + \mathcal{O}(1)$

5′. $\sum_{\chi} \overline{\chi(a)} \log L(s,\chi) = |\mathbb{Z}^{\star}(k)| \sum_{p \equiv a \mod k} \frac{1}{p^s} + \mathcal{O}(1)$

6′. $\sum_{\chi} \overline{\chi(a)} \log L(s,\chi) \to \infty$ as $s \to 1$

$\therefore \sum_{p \equiv a \mod k} \frac{1}{p}$ diverges.

Figure 5.1: A comparison of Euler's proof and the proof of Dirichlet's theorem.

tends to infinity as $s \to 1$. Thus $\sum_{p \equiv a \mod k} \frac{1}{p}$ must diverge and the proof of Dirichlet's theorem is completed. □

To help facilitate comparison with Euler's proof, both proofs are presented side by side in figure (5.1).

The characters are clearly crucial to the proof of Dirichlet's theorem. Indeed, their role is to pick out the primes in the relevant congruence class. However, as we saw, there are constraints on the way in which we can do this. In particular, we have to pick out the primes by making use of completely multiplicative functions, as we need to use the generalized Euler-Product formula. One of the most natural ways of picking out the primes, by making direct use of the indicator function $e_{a,k}$, is thus not available. However, Fourier analysis suggests a way to overcome this problem by representing the indicator function as a linear combination of better behaved, i.e. completely multiplicative, functions: the Dirichlet characters.

5.3 Dirichlet's Original Proof

The strategy Dirichlet used in his original proof is very similar to that outlined in section (5.2). However, some aspects of his approach are strikingly different, and, as I will argue

in section (5.4), they have consequences for the motivational efficacy of his proof. In this section, I will sketch Dirichlet's original proof, focusing on the treatment of characters.

Dirichlet broke his original proof up into two parts, first focusing on a simpler case before tackling the more general one. Thus in discussing Dirichlet's proof I will consider both the simple and more general cases separately.

5.3.1 The Simple Case

The simple version of Dirichlet's theorem restricts the common difference of the arithmetic progression to a prime:

Theorem 5.3.1 (Simple Case)**.** *Let q be a prime and suppose that q does not divide a. Then the arithmetic progression $a, a+q, a+2q, \ldots$ contains infinitely many primes.*

In order to understand Dirichlet's proof of this theorem, we first need to recall the definition of two different kinds primitive roots. First, we'll consider primitive roots mod q:

Definition Let q be a prime. Then a primitive root mod q is a number c such that for any $n \in \mathbb{Z}$, $q \nmid n$, there is $0 \leq \gamma_n \leq q-2$ such that $c^{\gamma_n} \equiv n \mod q$. γ_n is called the index of n to base c mod q.

For example, if $q = 7$ then 3 is a primitive root mod 7:

$3^0 \equiv 1 \mod 7$

$3^1 \equiv 3 \mod 7$

$3^2 = 9 \equiv 2 \mod 7$

$3^3 = 27 \equiv 6 \mod 7$

$3^4 = 81 \equiv 4 \mod 7$

$3^5 = 243 \equiv 5 \mod 7$

As every natural number n that is not divisible by 7 must be congruent to 1, 2, 3, 4, 5, or 6 mod 7, this means every n can be represented as power of 3 mod 7.

More generally, we have the following result about the existence of primitive roots mod q:

Theorem 5.3.2. *There is a primitive root for any odd prime q.*

Now recall the definition of a root of unity and a primitive root of unity:

Definition Let m be a natural number. Then $z \in \mathbb{C}$ is a mth root of unity if it satisfies the equation $x^m - 1 = 0$. An mth root of unity is a primitive root of unity if it is not a m'th root of unity for any $1 \leq m' < m$. In other words, a primitive mth root of unity, z, satisfies the equation $x^m - 1 = 0$ but does not satisfy $x^{m'} - 1 = 0$ for $1 \leq m' < m$.

Dirichlet used both of these notions of primitive roots to construct what we now call characters directly. Let c be a primitive root mod q and let Ω be a primitive $(q-1)$th root of unity. If n is an integer not divisible by q, denote by γ_n the index of n to base c mod q. Then Dirichlet wrote '$\Omega^{h\gamma_n}$', where $0 \leq h < q-2$ is a parameter that serves to distinguish between such expressions, whereas a modern author would write '$\chi(n)$'. Further, Dirichlet did not abbreviate these expressions, except to sometimes suppress the 'n' in 'γ_n'. Additionally, he did not use the term 'character' or identify the configuration $\Omega^{h\gamma_n}$ as the subject of mathematical study in its own right. Thus Dirichlet's treatment of what we now call characters in the simple case is already quite different from the presentation in the modern proof. Indeed, in the modern proof, information about the construction of the characters is not needed and is suppressed as far as possible. For example, recall that the characters were defined in terms of their properties (as group homomorphisms), not directly constructed. Moreover, it was their properties, not the details of their construction, that were referenced in the modern proof.[8]

Despite these differences, Dirichlet proceeded just like in the modern proof by showing that each $\Omega^{h\gamma_n}$ has an Euler Product formula. However, while the modern proof identifies this as a theorem and states it in a general manner, Dirichlet only proved a specialized form

[8]For a full discussion of the differences between the modern notion of character and Dirichlet's original, see (Avigad and Morris, 2014; Avigad and Morris).

of the result. More precisely, he argued that the following equation, where ω is any $(q-1)$th root of unity, holds:[9]

> ...
>
> $$\prod \frac{1}{1-\omega^{\gamma}\frac{1}{p^s}} = \sum \omega^{\gamma}\frac{1}{n^s} = L,$$
>
> where the multiplication sign applies to the whole series of primes with the only exception of q, while the sum is over all integers from 1 to ∞ not divisible by q. The letter γ means on the left γ_p, but on the right γ_n (Dirichlet, 1837a, 3).

These are Dirichlet's L-functions. Notice that there are $q-1$ of them, with one for each of the distinct $q-1$ roots of unity. Moreover, if Ω is a primitive $(q-1)$th root of unity, each $(q-1)$th root of unity can be written as a power of Ω. Dirichlet used these facts to introduce the notation $L_h = \sum \Omega^{h\gamma}\frac{1}{n^s}$.

Dirichlet proved the Euler Product formula directly by appealing to the properties of primitive roots mod q, indices and primitive $(q-1)$th roots of unity. Unlike modern authors, Dirichlet did not directly appeal to the complete multiplicativity of what we now call characters. That they are completely multiplicative, i.e. that for any n, n' coprime to q $\omega^{\gamma_{nn'}} = \omega^{\gamma_n}\omega^{\gamma_{n'}}$, is established by invoking properties of primitive roots mod q and their indices as well as $(q-1)$th roots of unity. This could then be appealed to in order to show that the Euler Product formula holds. However, Dirichlet opted to prove a more complex consequence of complete multiplicativity directly, and then use this to establish the Euler Product formula. Consequently his proof obscures one of the most important features behind the selection of the characters as presented in the modern proof: their complete multiplicativity.

With the Euler Product formula established, Dirichlet took logarithms of both sides. Assuming ω is any $(q-1)$th root of unity and further writing $s = 1+\rho$, where $\rho \in \mathbb{R}$, he obtained:

$$\sum \omega^{\gamma}\frac{1}{p^{1+\rho}} + \frac{1}{2}\sum \omega^{2\gamma}\frac{1}{p^{2+2\rho}} + \frac{1}{3}\sum \omega^{3\gamma}\frac{1}{p^{3+3\rho}} + \ldots = \log L \tag{5.1}$$

[9]Here and in other quotations that follow, I slightly change Dirichlet's notation for ease of comparison to the modern proof. In particular, Dirichlet considered an arithmetic progression with first term m and common difference p, a prime. Thus I replace 'm' with 'a' and interchange 'q' and 'p'.

Dirichlet's next move was to undertake steps 4' and 5' in figure (5.1) on page 81. I quote his exposition of these steps in full below. To aid comparison to the modern proof, note that if $\chi(n) = \Omega^{h\gamma_n}$ then $\overline{\chi(n)} = \Omega^{-h\gamma_n}$.

> If we multiply the equations contained in [equation 5.1] that correspond consecutively to the roots
>
> $$1, \Omega, \Omega^2, \ldots, \Omega^{q-2}$$
>
> with:
>
> $$1, \Omega^{-\gamma_a}, \Omega^{-2\gamma_a}, \ldots, \Omega^{-(q-2)\gamma_a}$$
>
> and add we get on the left hand side:
>
> $$\begin{aligned}
> &\sum (1 + \Omega^{\gamma-\gamma_a} + \Omega^{2(\gamma-\gamma_a)} + \ldots + \Omega^{(q-2)(\gamma-\gamma_a)}) \frac{1}{p^{1+\rho}} \\
> &+ \frac{1}{2} \sum (1 + \Omega^{2\gamma-\gamma_a} + \Omega^{2(2\gamma-\gamma_a)} + \ldots + \Omega^{(q-2)(2\gamma-\gamma_a)}) \frac{1}{p^{2+2\rho}} \\
> &+ \frac{1}{3} \sum (1 + \Omega^{3\gamma-\gamma_a} + \Omega^{2(3\gamma-\gamma_a)} + \ldots + \Omega^{(q-2)(3\gamma-\gamma_a)}) \frac{1}{p^{3+3\rho}} \\
> &+ \ldots
> \end{aligned}$$
>
> where the summation is over p and γ denotes the index of p. But now it holds that:
>
> $$1 + \Omega^{h\gamma-\gamma_a} + \Omega^{2(h\gamma-\gamma_a)} + \ldots + \Omega^{(q-2)(h\gamma-\gamma_a)} = 0,$$
>
> except when $h\gamma - \gamma_a \equiv 0 \mod q-1$, in which case the sum equals $q-1$. This congruence however is identical with $p^h \equiv a \mod q$. We therefore have the equation:
>
> $$\begin{aligned}
> &\sum \frac{1}{p^{1+\rho}} + \frac{1}{2} \sum \frac{1}{p^{2+2\rho}} + \frac{1}{3} \sum \frac{1}{p^{3+3\rho}} + \ldots \\
> &= \frac{1}{q-1} \left(\log L_0 + \Omega^{-\gamma_a} \log L_1 + \Omega^{-2\gamma_a} \log L_2 + \ldots + \Omega^{-(q-2)\gamma_a} \log L_{q-2} \right),
> \end{aligned}$$
>
> where the first summation is over all primes p of the form $\mu q + a$, the second over all primes p with squares of that form, the third over all primes p with cubes of

that form etc. (Dirichlet, 1837a, 13–14)

Note that the equation in the above quote,

$$1 + \Omega^{h\gamma-\gamma_a} + \Omega^{2(h\gamma-\gamma_a)} + \ldots + \Omega^{(q-2)(h\gamma-\gamma_a)} = \begin{cases} q-1 & \text{if } p^h \equiv a \mod q \\ 0 & \text{otherwise} \end{cases}$$

is Dirichlet's version of the modern equation

$$\sum_{\chi} \overline{\chi(a)}\chi(p^h) = |\mathbb{Z}^\star(q)| \cdot e_{a,q}(p^h).$$

While the modern proof identifies this as a crucial part of the proof, Dirichlet does not draw much attention to it. Indeed, he does not even identify it as a sub-result or a lemma.

Having already established that L_0, the L-function associated with the trivial character, tends to infinity as ρ tends to 0 and that, in addition, if $m > 0$ then L_m has a non-zero limit, Dirichlet could finish his proof. Indeed, these results allow him to conclude that the right hand side of

$$\begin{aligned} &\sum \frac{1}{p^{1+\rho}} + \frac{1}{2}\sum \frac{1}{p^{2+2\rho}} + \frac{1}{3}\sum \frac{1}{p^{3+2\rho}} + \ldots \\ &= \frac{1}{q-1}\left(\log L_0 + \Omega^{-\gamma_a}\log L_1 + \Omega^{-2\gamma_a}\log L_2 + \ldots + \Omega^{-(q-2)\gamma_a}\log L_{q-2}\right), \end{aligned}$$

tends to infinity as ρ tends to 0, which in turn allows him to conclude that the left hand side must tend to infinity. However, all of the sums on the left hand side, except the first, are bounded by a constant, and so $\sum \frac{1}{p^{1+\rho}}$ must tend to infinity as ρ tends to 0. Remembering that this sum ranges only over primes p of the form $\mu q + a$, theorem (5.3.1) follows. □

5.3.2 The General Case

Recall that, for the general case, Dirichlet wanted to establish that an arithmetic progression with first term a and common difference k, where a and k are coprime, contains infinitely many primes. His strategy is the same as in the simple case, but the construction of what we now call characters becomes more complex. In what follows I will sketch Dirichlet's

construction, before describing how such conglomerations are treated and used within the proof. For a full, modern exposition of Dirichlet's construction see Davenport (Davenport, 2013, chapter 3).

In the general case, just like in the simple case, Dirichlet constructs what we now call characters out of primitive roots and roots of unity. In the simple case, theorem (5.3.2) guarantees that there is a primitive root modulo the difference, q. This in turn means that, for any integer n coprime to q, there is some γ_n such that $c^{\gamma_n} \equiv n \mod q$. Theorem (5.3.2) generalizes to powers of odd primes:

Theorem 5.3.3. *If p is an odd prime and m is a natural number, then there is a primitive root mod p^m.*

However, it does *not* straightforwardly generalize for prime powers of the form 2^λ where $\lambda \geq 3$. Instead, the following result holds:

Theorem 5.3.4. *Let $\lambda \geq 3$. Then for any integer n coprime to 2^λ, there exist integers α_n, β_n such that $(-1)^{\alpha_n} 5^{\beta_n} \equiv n \mod 2^\lambda$*

Now consider the prime decomposition of the common difference of the arithmetic progression,

$$k = 2^\lambda q^\mu q'^{\mu'} \dots,$$

where $q, q', \dots$ are distinct odd primes. Theorems (5.3.3) and (5.3.4) tell us that, if n is coprime to k, then there are integers $\alpha_n, \beta_n, \gamma_n, \gamma'_n, \dots$ such that

$$(-1)^{\alpha_n} 5^{\beta_n} c^{\gamma_n} c'^{\gamma'_n} \dots \equiv n \mod k$$

where $c, c', \dots$ are the primitive roots modulo $q^\mu, q'^{\mu'}, \dots$ Then, by taking appropriate primitive roots of unity corresponding to the prime factors of k, Dirichlet wrote what is now recognized as the value of a general character as

$$\Theta^{\alpha_n \mathfrak{a}} \Phi^{\beta_n \mathfrak{b}} \Omega^{\gamma_n \mathfrak{c}} \Omega'^{\gamma'_n \mathfrak{c}'} \dots,$$

where $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \dots$ are parameters that serve to identify it. Thus, while a modern author writes

'$\chi(n)$' for an arbitrary character, Dirichlet wrote '$\Theta^{\alpha_n\mathfrak{a}}\Phi^{\beta_n\mathfrak{b}}\Omega^{\gamma_n\mathfrak{c}}\Omega'^{\gamma'_n\mathfrak{c}'}\ldots$' Just like in the simple case, Dirichlet often omitted the 'n' from the 'α_n', 'β_n', 'γ_n', 'γ'_n', ... However, he did not introduce further abbreviations for these conglomerations and referred to them in this way throughout his proof. This had a significant impact on its motivational efficacy.

As before, Dirichlet's first task was to establish an Euler Product formula. Assuming $\theta, \phi, \omega, \omega', \ldots$ are any suitable roots of unity, he demonstrated that the following equation holds:

$$\prod \frac{1}{1-\theta^{\alpha}\phi^{\beta}\omega^{\gamma}\omega'^{\gamma'}\ldots\frac{1}{p^s}} = \sum \theta^{\alpha}\phi^{\beta}\omega^{\gamma}\omega'^{\gamma'}\ldots\frac{1}{n^s} = L,$$

where the $\alpha, \beta, \gamma, \gamma', \ldots$ on the left hand side depend on p, while on the right they depend on n. There are $\phi(k)$ many such series and by making use of primitive roots of unity, $\Theta, \Phi, \Omega, \Omega', \ldots$, each of the series can be represented as

$$L_{\mathfrak{a},\mathfrak{b},\mathfrak{c},\mathfrak{c}',\ldots} = \sum \Theta^{\alpha_n\mathfrak{a}}\Phi^{\beta_n\mathfrak{b}}\Omega^{\gamma_n\mathfrak{c}}\Omega'^{\gamma'_n\mathfrak{c}'}\ldots\frac{1}{n^s}$$

for suitable integers $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{c}', \ldots$

In proving the Euler Product formula Dirichlet again did not refer to the complete multiplicativity of what we now call characters, instead invoking basic properties about primitive roots, indices and roots of unity. Thus again, the property of the characters that was central to the modern presentation is not mentioned in Dirichlet's proof.

With the Euler Product formula established, the next step was to take logarithms of each side, with s replaced by $1+\rho$:

$$\sum \theta^{\alpha}\phi^{\beta}\omega^{\gamma}\omega'^{\gamma'}\ldots\frac{1}{p^{1+\rho}} + \frac{1}{2}\sum \theta^{2\alpha}\phi^{2\beta}\omega^{2\gamma}\omega'^{2\gamma'}\ldots\frac{1}{p^{2+2\rho}} + \ldots = \log L. \tag{5.2}$$

With that established, Dirichlet again undertook analogues of steps 4' and 5' in figure (5.1). Making use of his notation $L_{\mathfrak{a},\mathfrak{b},\mathfrak{c},\mathfrak{c}',\ldots}$, he instructed the reader to multiply both sides of the corresponding equation (5.2) by $\Theta^{-\alpha_a\mathfrak{a}}\Phi^{-\beta_a\mathfrak{b}}\Omega^{-\gamma_a\mathfrak{c}}\Omega'^{-\gamma'_a\mathfrak{c}'}\ldots$ The general term of the left hand side then becomes

$$\frac{1}{h}\sum \Theta^{(h\alpha-\alpha_a)\mathfrak{a}}\Phi^{(h\beta-\beta_a)\mathfrak{b}}\Omega^{(h\gamma-\gamma_a)\mathfrak{c}}\Omega'^{(h\gamma'-\gamma'_a)\mathfrak{c}'}\ldots\frac{1}{p^{h+h\rho}}$$

while the right hand side becomes

$$\Theta^{-\alpha_a \mathfrak{a}} \Phi^{-\beta_a \mathfrak{b}} \Omega^{-\gamma_a \mathfrak{c}} \Omega'^{-\gamma'_a \mathfrak{c}'} \dots \log L_{\mathfrak{a},\mathfrak{b},\mathfrak{c},\mathfrak{c}',\dots}.$$

Next, Dirichlet took the sum over all of the combinations of roots of unity. He wrote:[10]

> ... the general term on the left hand side becomes:
>
> $$\frac{1}{h} \sum W \frac{1}{p^{h+h\rho}},$$
>
> where the sum is over all primes p and W means the product of the sums taken over $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{c}', \dots$ or respectively over:
>
> $$\sum \Theta^{(h\alpha-\alpha_a)\mathfrak{a}}, \sum \Phi^{(h\beta-\beta_a)\mathfrak{b}}, \sum \Omega^{(h\gamma-\gamma_a)\mathfrak{c}}, \sum \Omega'^{(h\gamma'-\gamma'_a)\mathfrak{c}'}, \dots$$
>
> We can now see ... that the first of these sums is 2 or 0, corresponding to if the congruence $h\alpha - \alpha_a \equiv 0 \mod 2$ or, equally, the congruence $p^h \equiv a \mod 4$ holds or not; that the second is $2^{\lambda-2}$ or 0 corresponding to whether the congruence $h\beta - \beta_a \equiv 0 \pmod{2^{\lambda-2}}$ or, equivalently, whether the congruence $p^h = \pm a \pmod{2^\lambda}$ holds or not; that the third is $(q-1)q^{\nu-1}$ or 0, corresponding to whether the congruence $h\gamma - \gamma_a \equiv 0 \pmod{(q-1)q^{\nu-1}}$ or, equivalently, whether the congruence $p^h \equiv a \pmod{q^\nu}$ holds or not, and so on; that therefore W always vanishes except when the congruence $p^h \equiv a \pmod{k}$ holds, in which case $W = K[= \phi(k)]$. (Dirichlet, 1837a, 20)

In the above passage, Dirichlet describes how what we now recognize as characters pick out the primes of the relevant congruence class. Thus the above paragraph was Dirichlet's way of expressing the modern equation

$$\sum_\chi \overline{\chi(a)} \chi(p^h) = |\mathbb{Z}^\star(k)| \cdot e_{a,k}(p^h).$$

[10] As before, I have replaced instances of 'q' by 'p' and vice versa. Additionally Dirichlet used 'π', 'π'', ... as the exponents of the primes in the decomposition of k. To avoid confusion for the modern reader, I have replaced these with 'ν'.

His version is *much* more difficult to parse, given the sheer amount of information that the reader must work through. Additionally, Dirichlet did not draw attention to the centrality of this result and, just like in the simple case, did not identify it as a sub-result or lemma.

However, with the above established, Dirichlet was able to simplify his equation and thus obtain:

$$\sum \frac{1}{p^{1+\rho}} + \frac{1}{2}\sum \frac{1}{p^{2+2\rho}} + \frac{1}{3}\sum \frac{1}{p^{3+3\rho}} + \dots$$
$$= \frac{1}{K}\sum \Theta^{-\alpha_a \mathfrak{a}} \Phi^{-\beta_a \mathfrak{b}} \Omega^{-\gamma_a \mathfrak{c}} \Omega'^{-\gamma'_a \mathfrak{c}'} \dots \log L_{\mathfrak{a},\mathfrak{b},\mathfrak{c},\mathfrak{c}',\dots}$$

The first sum on the left hand side ranges over all primes p of the form $a + \mu k$, the second sum ranges over all primes p whose squares are of that form, and the third ranges over all primes p whose cubes are of that form. The sum on the right hand side ranges over all $\phi(k)$ possible combinations of the integers $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{c}', \dots$

Assuming that $L_{0,0,0,\dots}$, the L-function corresponding to what we now call the trivial character, tends to infinity as ρ tends to 0 and that all other $L_{\mathfrak{a},\mathfrak{b},\mathfrak{c},\mathfrak{c}',\dots}$ have a non-zero limit as ρ tends to 0, Dirichlet's proof is completed. Indeed, putting everything together, we see that the right hand side of the above equation tends to infinity as ρ tends to 0. This means that the left hand side must do the same. However, all sums on the left hand side, except the first, are bounded by a constant. Consequently, $\sum \frac{1}{p^{1+\rho}}$ must tend to infinity as ρ tends to 0. But, recalling that this sum ranges over all primes p of the form $a+\mu k$, this establishes Dirichlet's theorem in the general case. □

5.4 An Analysis of the Motivational Efficacy of Dirichlet's Original Proof

5.4.1 Preliminary Remarks

Although the modern proof utilizes very similar ideas and insights to those found in Dirichlet's original, the proofs are nonetheless strikingly different. As I will argue, some of these differences have a negative impact on the motivational efficacy of his proof, and are difficult

to remedy given the context. In my analysis, I will be focused solely on the treatment of what are now called characters and will not discuss the more analytic features of the proof. However, the analytic components of the proof, which establish the non-vanishing of the L-functions, are a core part of the argument and contain deep mathematics. Thus while the characters form a crucial piece of Dirichlet's proof my analysis will be somewhat incomplete by neglecting the analytic side of his work.

Recall that in section (5.2), I tried to help the reader to identify the role that the characters play in the modern proof, as well as to grasp where they come from. In particular, I suggested that the role of the characters is to "pick out" primes of the relevant congruence class, which is achieved via theorem (5.2.5). Their introduction, on the other hand, is suggested by Fourier analysis. Indeed, a natural way to pick out the relevant primes would be to use the function $e_{a,k}$ directly, but this function fails to be completely multiplicative and thus does not have an Euler Product formula. Fourier analysis, however, provides a way of representing $e_{a,k}$ in terms of completely multiplicative functions: the characters. In other words, the modern presentation equips the reader with answers to the questions "What role do the characters play?" and "Where do they come from?" However, as I will argue in the next section, it is much more difficult for a reader of Dirichlet's proof to satisfactorily answer analogous questions.

5.4.2 Context

As I have argued in chapters 3 and 4, the motivational efficacy of a proof is context dependent. Thus, before analyzing Dirichlet's proof, I must specify a context. In doing so, I aim to be faithful to the mathematics of the time. More precisely, I aim to construct a context that reflects what a reader of the 1830s needs to know in order to check the correctness of the steps in Dirichlet's argument. However, the context I construct, below, is quite minimal, in the sense that it does not contain more than this.

The four components of this context are described below:

Resources

I am assuming that the context contains results about primitive roots modulo prime powers, for example, the existence of such roots and the properties that they and their indices possess, results about roots of unity and their properties and basic algebra. On the analytic side, I am assuming that the context includes tools from (real) analysis, relating to, for example, the convergence and divergence of series, tests for convergence etc. Importantly, I take the context to include an Eulerian style proof of the infinitude of the primes.

However, what the context does *not* contain is just as important as what it does include. First, although Dirichlet was intimately familiar with Fourier series[11], I will assume that it is not included within the context, as he made no reference to it in his proof. Second, I will assume that the generalized Euler Product formula is also missing from the context. Indeed, Dirichlet made no such reference to the result in his proof, and instead established directly that the series he was interested in had Euler Product formulas.

Further, I will assume that the context contains certain basic concepts and notations that are different to the standard modern ones. The concept of function is one such example, as the notion of function was less sharply defined in the 1830s than today. In particular, most instances of functions at that time were defined on a continuous domain, e.g. $\mathbb{R}$ or $\mathbb{C}$. Further, the earliest instance of the term 'number theoretic function' that Avigad and I found when investigating the history of the concept of function was due to Eistenstein in 1850 (Avigad and Morris, 2014, 6–7). Thus it is not clear that, in the 1830s, number theoretic functions were thought of as functions "proper". It is this less sharply defined concept of function that I take to be included within the context, rather than the fully modern one.

Similarly, it is important to realize that the treatment of mathematical entities, and the notation used to reflect this, was not as uniform in the 1830s as it is today. Today, for example, we use the same summation sign '$\sum$' to range over various different kinds of entities, from natural numbers, to group elements, to functions and so on. However, Dirichlet and other mathematicians did not use '$\sum$' in the same unrestricted manner, reserving it instead for familiar entities like the natural numbers. Indeed, Dirichlet introduced a new summation

[11]For example, Dirichlet rigorously proved that functions satisfying certain conditions converged to their Fourier series in 1829 (Dirichlet, 1829).

symbol, 'S', to range over all possible combinations of certain roots of unity in a 1841 paper generalizing his result about primes in arithmetic progressions (Dirichlet, 1841, 525). Similarly, de la Vallée Poussin, in his presentation of Dirichlet's theorem in 1897, used the symbol 'S' to represent the sum over all characters (de la Vallée Poussin, 1897, 20, 40, 48). Thus, again, I will be including the older, less uniform treatment of mathematical entities and the associated less uniform notation, in the context.

Structure

Dirichlet himself provided information that suggests a suitable structure for the context. First, as mentioned above, in his short paper announcing his theorem and sketching the proof, Dirichlet referenced Euler's proof of the infinitude of the primes (Dirichlet, 1837b, 309–310). This indicates that this proof should be close at hand within the context. Additionally, before giving his proof of the general case, Dirichlet collected together a number of important results concerning the existence of primitive roots and their properties: "... several theorems from the theory of residues will be necessary which we want to collect now to be able to refer to them more easily in the following. Justification of these results can be looked up in *Dis. arith. sec. III.* where the subject is treated in depth" (Dirichlet, 1837a, 14). This again suggests that these results should elevated to a privileged status in the context, so that they are easily accessible to the reader.

Conventions

I will not assume that there are any specific conventions in operation in the context, other than very general ones which are still in operation today. For example, I will assume the convention: Don't use standard resources in an unusual way, unless there is a good reason to do so. In practice, this convention means that if resources are extended within the given proof with no justification, then the step will fail to be appropriate. This may seem a very weak convention, but when other components of the context are taken into consideration, it makes it difficult to improve the motivational efficacy of Dirichlet's proof.

Values

In what follows I will not assume that there are any specific values in operation within the context. However, I would briefly like to discuss what happens if we add a value inspired by Kronecker: that when establishing the existence of a thing we also provide a method that produces the entity in question. If this is adopted as a value, Dirichlet's proof fails to respect it. As Kronecker explained "For the ambiguous characters [those which always have a real value], Dirichlet's proof meets this requirement [of producing the entity in question]. But his methods are not sufficient to do the same for the series corresponding to the complex characters [those characters which take at least one complex value]" (Kronecker and Hensel, 1901, 481). Some of the steps in Dirichlet's proof, therefore, fail to be appropriate in this Kroneckerian context and thus his proof fails to be motivated. Kronecker, however, offered a modified version of Dirichlet's proof that did respect this value.[12]

5.4.3 Analysis

Although I will ultimately argue that Dirichlet's original proof faces some motivational deficiencies when considered against the above context, there are a number of features of his proof which do help improve its motivational efficacy. First, Dirichlet's presentation helps the reader to ensure she has a suitably structured context, by indicating what is important, for example, the Eulerian style proof of the infinitude of the primes and the results about primitive roots. By doing this, Dirichlet ensured that the reader has certain key information ready to hand, which serves to reduce some of the cognitive burden she would suffer if her context was not set up in this manner.

Making the Eulerian style proof about the infinitude of the primes close to hand, in particular, has significant benefits. More specifically, it allows the reader to compare the new proof to one she already knows, thereby helping her to transfer knowledge of the old proof to the new one. This reduces her cognitive burden, as it reduces the amount of new information she must process. For example, she can exploit similarities between steps in the old and new proofs, and focus primarily on the differences between them. This will free up

[12]For more details about Kronecker's proof of Dirichlet's theorem, see (Avigad and Morris, 2014, 40–45).

more of her cognitive resources which she can then put towards grasping the appropriateness of the proof steps.

Drawing attention to an analogous proof can also help the reader to more directly recognize the appropriateness of the steps in the new proof. Indeed, if she knows what the role of a particular step in the old proof is, or if she knows where it comes from, then this should help her to grasp the role of the corresponding step in the new proof or where it comes from. Of course, there will still be work for the reader to do, particularly in figuring out how the differences between the old and new steps contribute to the proof. Additionally, if the reader fails to grasp the appropriateness of the steps in the old proof, then it will not necessarily put her in a favorable position for grasping the appropriateness of the steps in the new proof.[13]

Dirichlet's decision to break up his proof into two cases is also helpful. He broke the proof up not out of necessity, as it is possible to give the general proof without having first established the simple case, but to aid his readers: "With the novelty of the applied principles it appeared useful to me to start with the treatment of the special case where the difference of the progression is an odd prime, before proving the theorem in its entire generality" (Dirichlet, 1837a, 2). The simple case places fewer demands on the cognitive resources of the reader, given that there is much less information to parse, and thus helps her to grasp the strategy and structure of the proof. While I will argue, later, that she is still not in a favorable position to fully grasp the appropriateness of some of the steps, she is in a better position to determine the important ingredients in the argument compared to if Dirichlet had only given the general proof. Thus breaking the proof up into two parts helps place the reader in a better position to partially, though not fully, grasp the appropriateness of the steps.

However, as I mentioned above, Dirichlet's proof also has features which serve to diminish its motivational efficacy. One of the main difficulties with the proof is the sheer amount of information that the reader must parse. Even in the simple case, the reader has to keep track of a lot of data pertaining to what we now call characters. For while at first Dirichlet's notation '$\Omega^{h\gamma_n}$' is not too bad compared to the modern '$\chi(n)$', the data that must be kept track of in-

[13]However, sometimes seeing a similar step being used in two different situations can help to reveal salient commonalities that can help the reader to grasp their appropriateness.

creases quickly. For example, Dirichlet multiplied equations by $1, \Omega^{-\gamma_a}, \Omega^{-2\gamma_a}, \ldots, \Omega^{-(q-2)\gamma_a}$ and added the results, yielding equations such as $1+\Omega^{h\gamma-\gamma_a}+\Omega^{2(h\gamma-\gamma_a)}+\ldots+\Omega^{(q-2)(h\gamma-\gamma_a)}$. In modern terms, that equation gets represented as $\sum_\chi \overline{\chi(a)}\chi(p^h)$, which is much more concise and yet provides all the information that is needed.

The situation is far worse in the general case, as much more data is needed to refer to what we now call the characters, which Dirichlet wrote as $\Theta^{\alpha_n \mathfrak{a}}\Phi^{\beta_n \mathfrak{b}}\Omega^{\gamma_n \mathfrak{c}}\Omega'^{\gamma'_n \mathfrak{c}'} \ldots$ And, as we have seen, when he needed to perform operations on these conglomerations, the resulting expressions became even more difficult to manage. Indeed, in places Dirichlet had to resort to using natural language to describe the mathematics.

Ultimately, the "data richness" of Dirichlet's proof demands a significant portion of the reader's attention. This means that she has less cognitive resources available to devote to searching for the role that the particular steps play in the proof or where they come from. Consequently, she is not in a favorable position to grasp the appropriateness of the steps in the proof.

The lack of structure in parts of Dirichlet's proof also compounds the difficulty posed by the data rich presentation. For while Dirichlet did break his proof up into a simple and a general case and further placed the crucial results about the non-vanishing of L-functions in separate sections, his treatment of what are now called characters was not well structured. Recall, for example, that Dirichlet proved the Euler Product formula for his L-functions separately in both proofs, without separating out a general version or appealing to complete multiplicativity. Similarly, Dirichlet did not separately identify his versions of the core modern result $\sum_\chi \overline{\chi(a)}\chi(p^h) = |\mathbb{Z}^\star(k)| \cdot e_{a,k}(p^h)$. Instead, he established them as and when he needed them in the body of his main proof. His presentation in the general case is particularly problematic, because the statement of the result itself is buried within a wordy proof.

With these general features in mind, I will now focus on individual steps in Dirichlet's proof. In particular, I will focus on the step in which what we now call characters first appear: the introduction of the Euler Product formula. A reader may ask "What role does this step play in the proof?" and "Where does this step in the proof come from?" I will consider the question of the role of the Euler Product in the proof of the simple case first. Referring

to the Eulerian style proof of the infinitude of the primes, the reader should recognize that the original Euler Product provided a way to relate the series of interest, $\sum_p \frac{1}{p}$, to a more familiar sum over natural numbers that is easier to work with. Of course, the Euler Product was only the first step, and the series had to be extracted by taking logarithms, using Taylor series expansions and taking limits, but it was the hook upon which these later operations depended. With this in mind, the reader should realize that the more general Euler Product formula that Dirichlet proved in the simple case serves a similar purpose by allowing him to connect the series of interest, in modern terms $\sum_{p \equiv a \mod q} \frac{1}{p}$, to a sum over natural numbers. Moreover, given these differences, she should suspect that the expressions $\Omega^{h\gamma_n}$ relate to the extraction of the more complicated series. This is confirmed by Dirichlet's equation

$$1 + \Omega^{h\gamma - \gamma_a} + \Omega^{2(h\gamma - \gamma_a)} + \ldots + \Omega^{(q-2)(h\gamma - \gamma_a)} = \begin{cases} q-1 & \text{if } p^h \equiv a \mod q \\ 0 & \text{otherwise} \end{cases}$$

Thus she should reasonably be expected to grasp that the primary role these conglomerations play is in "picking out" primes in the relevant congruence class. Nonetheless, while she should recognize this, it is not entirely straightforward. Indeed, the data rich nature of Dirichlet's proof and its lack of structure potentially obscure some of these connections. Thus, while the step is recognizably contribution appropriate, it is not easily recognizable.

The question of "where does this step come from?" is harder to answer. Certainly, the reader can appeal to the corresponding step in the Eulerian style proof of the infinitude of the primes and the similarity of the tasks at hand, but she then needs to focus on the conglomerations $\Omega^{h\gamma_n}$ themselves. Clearly, the answer I sketched at the end of section (5.2) is not available; after all, the context does not contain Fourier analysis. But, even if it did, it would be difficult for the reader to grasp the connection without recognizing the conditions under which the Euler Product formula holds more generally, i.e. the requirement of complete multiplicativity, which Dirichlet did not formulate. Of course, that *this* answer is not available does not mean there are *no* satisfactory answers, but it is difficult to imagine one given the relatively restricted resources in the current context.[14] Thus while the step

[14]If the context is extended a little more to include cyclotomy and the theory of equations, then there may be a satisfactory answer. Avigad and I, for example, suggest that Dirichlet's proof may have been inspired by Lagrange's work on the theory of equations and, in particular, the Lagrange resolvent (Avigad

is partially introduction appropriate and should be recognized as such by the reader, it is not completely so. Indeed, the reader should not be expected to discover a fully satisfactory answer to the question "where do the characters come from?" on her own.

I will now consider the introduction of the Euler Product formula in the general case, assuming that the reader has consumed the proof of the simple case of Dirichlet's theorem. As the reader can answer the question of how the Euler Product formula advances the argument in the simple case, she should be in a favorable position to grasp its role in the general case, too. In particular, the only difference between the steps is the complexity of what we now call characters, but with their role in the simple case close to hand, the reader should be able to check that the more complicated expressions play the same role. However, again the data richness of the presentation and its lack of structure mean that this task requires considerable cognitive resources. Consequently, while the step is contribution appropriate and recognizably so, it is not easily recognizable.

The knowledge the reader has of the simple case can also help her to partially answer the question of "where does this Euler Product formula come from?" Indeed, given the simpler version of the Euler Product formula, she should be expected to recognize how those conglomerations can be generalized to the more complex case. Thus the reader should be expected to answer the question "where does this come from?" *relative to the first proof.* However, this is *not* a complete answer, as a satisfactory answer to the question of where the simpler conglomerations come from is not available. Thus, like in the simpler case, the Euler Product formula in the general case is only partially recognizably introduction appropriate.

In conclusion, Dirichlet's data-rich, non-modular presentation of the characters partially obscures the role that they play in the proof. Further, the lack of resources in the context make it unlikely that an answer to the question "Where do these conglomerations come from?" is available. Indeed, even if such an answer were available, Dirichlet's presentation would make it difficult for the reader to uncover it.

and Morris, Appendix). Thus could, in turn, provide an alternative answer to the question "Where do the characters come from?".

5.4.4 Increasing Motivation

It is tempting to think that a few small changes could overcome most of the motivational difficulties that Dirichlet's proof faces. Indeed, given that the data rich presentation and the lack of structure have a significant and negative impact on its motivational efficacy, a modern proof editor might think that it is easy to "fix up" Dirichlet's proof without requiring any significant changes to the context. However, this is not the case.

Suppose, for example, that a modern proof editor proposes to increase the motivational efficacy of the proof by making it more modular. He may first decide to treat the conglomerations that we now recognize as characters as particular kinds of functions, as this would provide a way to abbreviate them and thus reduce the amount of data the reader must keep in mind. Parts of the proof would still depend on the manner in which they are constructed, however, such as the representation of the indicator function. Thus the editor may suggest that these are "broken out" from the main proof, established separately and then referred to when needed in the main proof. This would further reduce the data required for the main proof and, in addition, would thus help to improve its structure by identifying sub-results that are important to the proof.

Moreover, the editor may suggest changing the manner in which Dirichlet denotes sums over what we now call characters. For example, recall that in the simple case, Dirichlet only abbreviated such sums by use of an ellipsis. Thus his work contained expressions such as $1 + \Omega^{h\gamma-\gamma_a} + \Omega^{2(h\gamma-\gamma_a)} + \ldots + \Omega^{(q-2)(h\gamma-\gamma_a)}$. In the general case, Dirichlet did make use of a summation sign, but this ranged over the series of integers used to distinguish the conglomerations from each other: $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{c}', \ldots$ Thus complicated expressions such as $\sum \Theta^{-\alpha_a \mathfrak{a}} \Phi^{-\beta_a \mathfrak{b}} \Omega^{-\gamma_a \mathfrak{c}} \Omega'^{-\gamma'_a \mathfrak{c}'} \ldots \log L_{\mathfrak{a},\mathfrak{b},\mathfrak{c},\mathfrak{c}',\ldots}$ appeared in his work. However, treating these conglomerations as functions suggests using a summation sign that ranges over them directly: '$\sum_\chi$'. This provides a further way in which the data in the proof reduced or hidden.

While these suggestions would indeed reduce the amount of information that a reader needs to keep track of, they would not serve to make Dirichlet's proof better motivated when considered against the context described in section (5.4.2). First, treating the conglomerations as functions breaks an important convention in the context: don't use stan-

dard resources in an unusual way (without "good" reason). Recall that when describing the context, I noted that the concept of function used in the 1830s was more restrictive and less well defined than the modern concept, with most functions being defined on continuous domains. Thus it is not clear that Dirichlet's conglomerations, being dependent on the elements of a discrete domain, count as "proper" functions. While the conception of function did eventually widen, it was a process that took time and effort. Indeed, when expanding a mathematical concept, mathematicians have to ensure that they have suitable rules for using the newly extended concept, and must be confident that these rules will not lead to conflicts with other, existing areas of mathematics (Avigad and Morris, §2). Thus even though treating Dirichlet's conglomerations as functions provides certain benefits to his proof, it is not justified with respect to this context. More specifically, treating them like this would make the proof steps inappropriate with respect to the context.

A similar difficulty arises with the use of the notation '$\sum_\chi$', even if treating Dirichlet's conglomerations as functions was unproblematic. Indeed, as mentioned in section (5.4.2), Dirichlet and other authors of the time used the notation '$\sum$' for sums ranging over (subsets of) the integers, rather than more exotic entities, a practice which continued at least until 1897. Thus letting the summation sign, '$\sum$', range directly over the characters violates the convention of not stretching standard resources, and hence steps that contain that notation would fail to be appropriate with respect to the context. Of course, this could be overcome by showing that stretching the notation is harmless and beneficial, but that requires additional work to augment the context.

Thus, while a modern proof editor will find it easy to "fix up" Dirichlet's proof, these changes would not be acceptable unless we also update the context. Moreover, it only seems easy, from a modern perspective, to suggest these changes because mathematicians before us have grappled with difficult questions concerning the nature of mathematical entities and how they should be treated. Indeed, when Dirichlet introduced the conglomerations that we now call characters for the first time in his 1837 proof, he faced difficult questions: "How should these entities be understood?" and "How should they be treated?" In his proofs, he opted for the safest answer, taking them to be nothing more and nothing less than the sum of their parts, which were well understood and had clear rules of operation. This does have a

cost, however, as we have seen: the resulting mathematics is clunky and difficult to control. In other words, the associated presentation is somewhat ineffective. This, in turn, made it more difficult for Dirichlet to transmit his knowledge to the mathematical community via a motivated proof.

However, these tricky questions arise again when further generalizations of Dirichlet's conglomerations were found to be useful, but even more difficult to control. For example, Dirichlet generalized his theorem to arithmetic progressions in the Gaussian integers in 1841 and in doing so introduced expressions of the form

$$\phi^{\alpha_n}\phi'^{\alpha'_n}\ldots\times\psi^{\beta_n}\chi^{\gamma_n}\psi'^{\beta'_n}\chi'^{\gamma'_n}\ldots\times\theta^{\delta_n}\eta^{\epsilon_n}$$

where $\phi, \phi', \psi, \psi', \chi, \chi', \theta, \eta$ are all roots of unity and $\alpha_n, \alpha'_n, \beta_n, \beta'_n, \chi_n, \chi'_n, \ldots, \delta_n, \epsilon_n$ are indices with respect to n. It is telling that in his 1841 paper, Dirichlet abbreviated these conglomerations to Ω_n, identified the core properties that they satisfy, and introduced a new notation for summing over them. Indeed, it indicates that he recognized his previous answers to the questions of how to understand and treat such entities were becoming less viable.

More generally, situations similar to this one forced mathematicians to re-evaluate how Dirichlet's conglomerations were conceived and treated, and consequently, to re-evaluate other elements of their context, too. Thus we have a case in which the ineffectiveness of certain presentations caused a re-conceptualization of particular mathematical entities. However, in the case of the characters this was a slow process: it took nearly 100 years for the fully modern conception to emerge.[15]

It should not be surprising that these changes took a considerable amount of time. Indeed, some of the changes that took place involved central concepts, such as that of "function". When changes are made to resources that are heavily used in other areas of mathematics, we must take care of any readjustments that are required in those areas, too. Further, if we are to make significant changes to the context against which a proof is considered, we ought to consider the impact that it will have on other proofs. We do not, for example, want to make changes that improve the motivational efficacy of one proof, but diminish the

[15]Full details of the transformation are discussed at length in my masters thesis (Morris, 2011) and joint papers with Avigad (Avigad and Morris, 2014; Avigad and Morris).

motivational power of others. Moreover, even if changing the context does not decrease the motivational efficacy of other proofs, we ought to ask ourselves if the benefits of the changes are worth it. Indeed, making changes to a given mathematical context costs time and effort. If the increase in motivational efficacy it provides is only minimal, our time and effort will be better spent elsewhere.

Consequently, while Dirichlet's proof is not particularly well motivated when considered with respect to the original context, improving it is not an easy process. Indeed, significant improvements in motivational efficacy require mathematicians to grapple with difficult questions concerning the nature of our mathematical entities.

Chapter 6

Motivation and Other Virtues

6.1 Preliminary Remarks

In section (2.3.2) I briefly discussed the connection between motivated proofs and proofs which possess other virtues, such as being explanatory or being non-arbitrary. I suggested that, while motivated proofs may seem similar to these other kinds of desirable proofs, there is reason to think that they are distinct and worthy of separate investigation. Now that I have presented my account of motivated proofs, I can return to these issues in greater detail.

6.2 Kitcher

Let P be a proof which is being considered with respect to a context C. Recall that P is well motivated with respect to C if and only if each step in P is recognizably correct and recognizably appropriate with respect to C. On Kitcher's theory, P will count as a successful explanation if and only if it is a member of the explanatory store $E(K)$, which I'll describe below, for its domain K. Recall that K is assumed to be a consistent and deductively closed set of beliefs that an idealized mathematical community would accept. $E(K)$ is then the most unifying systematization of K, i.e. the systematization that maximizes the number of conclusions drawn while minimizing the number of (genuine) argument patterns used (see e.g. (Kitcher, 1989, 431)).

I will argue that Kitcher's account of explanation and my account of motivation do not

pick out the same class of proofs. To do this, however, I must first determine a suitable domain, K. The context C cannot serve as the domain K because they are different types of entities. Indeed, the context has structure, which a set of beliefs lacks. Further, the definitions and theorems that make up the resources of the context are not assumed to be deductively closed. However, taking K to be the deductive closure of the set of definitions and theorems included within the context allows for a suitable comparison. Having decided upon a suitable K, the next task is to determine the explanatory store, $E(K)$. The description of the selection of $E(K)$, below, follows Kitcher (Kitcher, 1989, 434–435).

The explanatory store is the "best", i.e. most unifying, systematization of K. A *systematization* of K is simply a set of derivations, whose premises and conclusion are all elements of K. However, some systematizations ought to be excluded, such as those which include arguments that are not deductively valid, or which include premises not contained in K. Kitcher calls systematizations that are not excluded for these reasons *acceptable* relative to K. In order to compare the unifying power of the acceptable systematizations, Kitcher brings in the notion of generating sets, which are made up of schematic arguments or argument "patterns". More precisely, if S is an acceptable systematization, then G is a *generating set* for S if each derivation in S instantiates an argument pattern in G. However, a further condition on generating sets is required to ensure that all instantiations of a particular pattern have the same explanatory value, i.e. to rule out cases where one instantiation is deemed explanatory but not another. The additional condition is as follows: each derivation that instantiates a pattern in the generating set G and is acceptable relative to K is also contained in S. A generating set that meets this condition is said to be *complete*.

The next task in identifying $E(K)$ is to select a *basis* for each acceptable systematization. A basis for an acceptable systematization is a complete generating set that is most unifying, in the sense of minimizing the number of argument patterns used, while maximizing the number of conclusions drawn (assuming that the argument patterns are genuine and not gerrymandered).[1] Finally the bases for different acceptable systematizations are compared. The systematization associated with the basis that achieves the best tradeoff between the

[1]Kitcher calls genuine patterns "stringent". However, as there are difficulties with his account of stringency (Hafner and Mancosu, 2008a), I will not discuss it in detail here.

number of (genuine) argument patterns used and conclusions drawn is then the explanatory store $E(K)$.

Having now characterized $E(K)$ more precisely, I will return to the question of whether motivated proofs just are explanatory ones. For this claim to be correct, the following condition must hold:

> Given any proof P and context C, P is in $E(K)$ if and only if each step of P is recognizably correct and recognizably appropriate with respect to C.

I have argued that the structure of the context, for example, what resources are privileged and thus easily accessible, as well as the conventions or values in operation can affect the degree to which a proof step is recognizably correct or recognizably appropriate. $E(K)$, however, is obtained by finding the least number of (legitimate) patterns that allow the greatest number of conclusions to be derived. Thus recognizable correctness and appropriateness, on the one hand, and explanatoriness, on the other, are sensitive to different kinds of information. It may be possible, then, to use these differences to obtain a proof that is motivated but not explanatory, or explanatory but not motivated. Hafner and Mancosu's careful analysis of Kitcher's theory of explanation provides some potential examples of such proofs (Hafner and Mancosu, 2008a).

More specifically, Hafner and Mancosu apply Kitcher's theory to a case study from real algebraic geometry. They consider three proof methods and associated systematizations of the theory of real closed fields (RCFs).[2] The first proof method relies on the existence of a decision procedure for RCFs: a procedure which, given any elementary sentence ϕ, outputs the value 1 if RCF proves ϕ and 0 if it proves $\neg\phi$. The second proof method relies on the completeness of RCF, which has the following "transfer principle" as a consequence: if ϕ is true in one particular RCF, then it must be true in *all* RCFs. Thus to prove a theorem by this method, a mathematician establishes that it is true in a convenient RCF and then appeals to the transfer principle. The third proof method uses non-elementary techniques but avoids the use of the "transfer principle" (for more details, see (Hafner and Mancosu, 2008b, 161–165)).

[2]However, each of the systematizations goes beyond the theory of RCF.

The crucial point to note for present purposes is that the "best" systematization of the domain is the one which relies on the existence of the decision procedure, because it can be obtained with only one argument pattern.[3] Thus proofs that instantiate this argument pattern are successful explanations, while others are not (as) explanatory on Kitcher's theory. However, as Hafner and Mancosu point out, proofs obtained in this manner can be problematic. They quote the mathematician Gregory Brumfiel who notes that such proofs "...certainly might be very tedious, if not physically impossible, to work out ..." (Hafner and Mancosu, 2005, 159). In other words, proofs that are carried out in this manner may be subject to information management issues, and, as I suggested in previous chapters, this has a negative impact on the motivational efficacy of a proof regardless of context. Thus a suitably long proof of this form will provide an example of a proof that is explanatory on Kitcher's theory but not well motivated. On the other hand, a proof obtained by one of the alternative methods will not be (as) explanatory for Kitcher. Yet as mathematicians favor using these alternative methods themselves, there are non-artificial contexts against which such proofs are well motivated. Take, for example, one of Brumfiel's proofs using the third proof method. Then we can take the context to be as described by his book up until that point. As Brumfiel was sensitive to the benefits and drawbacks of each of the three proof methods Hafner and Mancosu discuss, his proof will presumably be well motivated with respect to this context. However, it will not be (very) explanatory for Kitcher, as it does not belong to the explanatory store.

It should be noted that Hafner and Mancosu are arguing that Kitcher's theory fails to provide a satisfactory account of mathematical explanation. Refining Kitcher's theory so as to better account for mathematical explanation may change the best systematization in the real algebraic geometry case study, and thus undermine my potential examples of motivated but not explanatory and explanatory but not motivated proofs. However, the core difference between my account of motivated proofs and Kitcher's account of explanatory proofs consists in the type of information that they are sensitive to. To be faithful to its guiding idea of unification, Kitcher's account must focus on a trade off between the conclusions that can be derived and the number of patterns that must be remembered. My account, however,

[3]The other systematizations Hafner and Mancosu focus on require infinitely many argument patterns.

considers a proof with respect to a particular, fixed context, and examines to what extent the structure of the context, conventions and values in operation help or hinder the reader to grasp where the steps come from and how they advance the argument. Thus although a refined version of Kitcher's theory may be developed, I suggest that other candidate proofs that are explanatory but not well motivated and vice versa could be found.

However, Kitcher's theory of explanation does complement the account of motivated proofs I develop in the following way. Kitcher's procedure for identifying the explanatory store for a domain may provide insight into how to best structure our mathematical contexts. In particular, examining the argument patterns that generate the explanatory store may suggest which concepts or techniques are particularly useful or fundamental in the theory. If these tools are given a privileged position within the context and are utilized within new proofs the reader is exposed to, the reader should be in an improved position from which to recognize the correctness and appropriateness of the proof steps. That is to say, Kitcher's theory may suggest a way to structure the context so as to promote well motivated proofs.

6.3 Steiner

Recall that, for Steiner, an explanatory proof is one which clearly depends on a "characterizing property" of an entity mentioned in the theorem and, further, is generalizable. By 'generalizable', Steiner means that "One must be able to generate new, related proofs by varying the [characteristic] property and reasoning again" (**?**, 151, endnote 11). Thus, at first glance, Steiner's account appears to have some commonalities with my account of motivated proofs. Indeed, the requirement that the proof depend clearly on the characterizing property is similar to the requirement that the reader recognize the correctness and appropriateness of the steps in a motivated proof. Further, the demand that explanatory proofs be generalizable connects to reuseability, and thus to one of the important consequences of motivated proofs. However, there are significant differences between the two accounts.

I suggested in section (2.3.2) that certain proofs by induction are candidates for motivated but non-explanatory proofs on Steiner's account. For example, Steiner claims that the standard inductive proof given to show that the sum of the first n positive consecutive

integers is $\frac{1}{2}n(n+1)$ fails to be explanatory. This proof is given below:

Theorem 6.3.1. $\sum_{i=1}^{n} i = \frac{1}{2}n(n+1)$

Proof. First consider the base case. $\sum_{i=1}^{1} i = 1 = \frac{1}{2}1(1+1)$. Thus the result holds when $n = 1$.

Next consider the induction step. Suppose that $\sum_{i=1}^{n} i = \frac{1}{2}n(n+1)$. It is to be shown that $\sum_{i=1}^{n+1} i = \frac{1}{2}(n+1)(n+2)$.

$$\sum_{i=1}^{n+1} i = \left(\sum_{i=1}^{n} i\right) + (n+1) \tag{6.1}$$

$$= \frac{1}{2}n(n+1) + (n+1) \text{ by IH} \tag{6.2}$$

$$= \frac{1}{2}n(n+1) + \frac{1}{2}2(n+1) \tag{6.3}$$

$$= \frac{1}{2}(n+1)(n+2) \tag{6.4}$$

□

Steiner supports his claim that the above proof is not explanatory in two ways. First, he argues that the inductive proof fails to make use of a characterizing property. Second, he claims that inductive proofs are not generalizable: "Inductive proofs usually do not allow deformation, since before one reasons one must have already conjectured the theorem" (**?**, 151, endnote 11).

However, given a standard context comprising of elementary number theory and algebra, it seems reasonable to conclude that such a proof will be motivated. After all, a reader with access to such a context should reasonably be expected to answer the questions "What role does each step play?" and "Where does each step come from?" Indeed, the role and reasons for introduction of some of the steps are (almost) given to the reader for free once she recognizes the use of the proof technique. For example, the role of the base case, $\sum_{i=1}^{1} i = 1 = \frac{1}{2}1(1+1)$, is to provide a starting point for the induction. Further, it comes from instantiating the induction technique for the theorem under consideration. Some of the steps in the rest of the proof need further clarification, but answers to the corresponding

questions should be easy to find. For example, the role of step 6.2 is to express $\sum_{i=1}^{n+1} i$ as a polynomial in n. As to the question of where it comes from, very little ingenuity is required. Indeed, the reader can recognize that the induction hypothesis expresses the smaller sum $\sum_{i=1}^{n} i$ as a polynomial in n, and the relationship between $\sum_{i=1}^{n} i$ and $\sum_{i=1}^{n+1} i$ suggests step 6.2 almost immediately. Consequently this proof provides an example of a motivated (relative to the context) proof that fails to be explanatory according to Steiner's theory. Thus there is reason to think motivated proofs are not the same as explanatory proofs, at least not as understood by Steiner.

More generally, note that Steiner's remarks about this proof apply to many other proofs by induction. Thus Steiner is declaring that many (most?) instances of a given proof technique are non-explanatory. This is a very strong claim and one which is at odds with a core feature of my account of motivated proofs: contextual dependence.

Finally, while explanatory proofs are re-useable on Steiner's account, they are only so in a very particular, restrictive way. Their re-useability comes from their generalizability, which requires that they are "deformable" into other proofs by varying the characteristic property but following the same reasoning. As Steiner makes clear when discussing inductive proofs, mathematicians should not have to make new conjectures as part of the deformation process (**?**, 151). Thus the re-useability associated with Steiner's explanatory proofs is of a very "immediate" and restrictive type. The re-useability I refer to as a benefit of motivated proofs is of a less specific, more general type. More precisely, motivated proofs help the reader to make and evaluate mathematical analogies. This, in turn, should help her to become more efficient in finding her own proofs.

6.4 Sandborg

Sandborg is the only philosopher I know of who has tackled the issue of motivated proofs explicitly. As mentioned in section (2.3.2), he connects motivation to non-arbitrariness, which he takes to be an explanatory virtue. Recall that, for Sandborg, a step appears arbitrary when a reader cannot see why it was selected compared to other possibilities. Thus to reduce arbitrariness, a proof author or editor should provide a reason for selecting

the step over other possibilities. To do this, Sandborg maintains that a favorable property should be identified and the selected step shown, or at least suggested, to have that property while (most) of the other possibilities are shown, or at least suggested, to lack it. Further, this must be done in a manner which satisfies two constraints (Sandborg, 1998, 148–149): (i) the possibilities are represented generically; (ii) the possibilities are compared with respect to the favorable property in a uniform manner.

Sandborg applies his account of non-arbitrariness to Pólya's discussion of Carleman's inequality (see sections 2.1.1 and 2.3.2). Recall that Pólya's proof contained a "deux ex machina" in the form of an auxiliary sequence. While this made the proof work almost magically, Pólya held that it would leave the reader unsatisfied. He thus added additional material designed to relieve the sense of dissatisfaction that it created. On Sandborg's analysis, the additional material was *not* successful at reducing the arbitrariness associated with the *strategy* of using an auxiliary sequence, as condition (ii) is not satisfied. However, he claimed that it was more successful at reducing the arbitrariness associated with the selection of the *particular* sequence. On my account of motivation, Pólya's material relating to the introduction of the proof strategy is more successful. To compare my account and Sandborg's, I will now present Pólya's considerations in more detail.

Recall that Carleman's inequality is the following theorem (Pólya, 1949, 684):

Theorem 6.4.1. *If $a_1, a_2, \ldots$ are real, non-negative numbers and are not all equal to 0, then the following inequality holds:*

$$\sum_{n=1}^{\infty}(a_1 a_2 \ldots a_n)^{\frac{1}{n}} < e\sum_{n=1}^{\infty} a_n.$$

Pólya's proof relies on the Arithmetic-Geometric Mean Inequality:

Theorem 6.4.2 (Arithmetic-Geometric Mean Inequality)**.** *Suppose that $x_1, x_2, \ldots x_n$ is a sequence of non-negative reals. Then*

$$(x_1 x_2 \ldots x_n)^{\frac{1}{n}} \leq \frac{x_1 + x_2 + \ldots + x_n}{n}$$

with equality holding if and only if $x_1 = x_2 \ldots = x_n$.

Pólya's (unmotivated) proof of Carelman's inequality, along with his additional motivational material, is presented below (Pólya, 1949, 684–690):

Proof. Define a sequence $c_1, c_2, \ldots$ such that

$$c_1 c_2 c_3 \ldots c_n = (n+1)^n.$$

Now note that

$$\sum_{n=1}^{\infty} (a_1 a_2 \ldots a_n)^{\frac{1}{n}} = \sum_{n=1}^{\infty} \frac{(a_1 c_1 a_2 c_2 \ldots a_n c_n)^{\frac{1}{n}}}{n+1}$$

and apply the Arithmetic Geometric Mean Inequality. This yields

$$\begin{aligned}
\sum_{n=1}^{\infty} \frac{(a_1 c_1 a_2 c_2 \ldots a_n c_n)^{\frac{1}{n}}}{n+1} &\leq \sum_{n=1}^{\infty} \frac{a_1 c_1 + a_2 c_2 + \ldots + a_n c_n}{n(n+1)} \\
&= \sum_{k=1}^{\infty} a_k c_k \sum_{n \geq k} \frac{1}{n(n+1)} \\
&= \sum_{k=1}^{\infty} a_k c_k \sum_{n \geq k} \left(\frac{1}{n} - \frac{1}{n+1} \right) \\
&= \sum_{k=1}^{\infty} a_k \frac{(k+1)^k}{k^{k-1}} \frac{1}{k} \\
&< e \sum_{k=1}^{\infty} a_k
\end{aligned}$$

□

Pólya then augments his proof with motivational material which consists of a number of "false starts" to proving the theorem. Pólya analyzes these attempts to identify the likely cause of the failure and suggests ways of fixing them, which eventually result in a working proof. I'll focus on just the first false start here, as this is where the primary disagreement between Sandborg's account and my own arises.

In the additional material, Pólya explains that Carleman's inequality is used to establish another result: assuming that a_i is a sequence of positive real numbers, then if $\sum_{n=1}^{\infty} a_n$ converges, $\sum_{n=1}^{\infty} (a_1 a_2 \ldots a_n)^{\frac{1}{n}}$ must also converge. In rough terms, this means that $(a_1 a_2 \ldots a_n)^{\frac{1}{n}}$

must remain small, assuming that $a_1+a_2+\ldots+a_n$ is not large. This immediately (via pattern-matching) suggests using the Arithmetic-Geometric Mean Inequality. However, when the reader tries this approach, she will run into difficulties (see (Pólya, 1949, 687)):

$$\begin{aligned}\sum_{n=1}^{\infty}(a_1a_2\ldots a_n)^{\frac{1}{n}} &\leq \sum_{n=1}^{\infty}\frac{a_1+a_2+\ldots+a_n}{n}\\ &= \sum_{n=1}^{\infty}a_k\sum_{n=k}^{\infty}\frac{1}{n}\end{aligned}$$

The trouble here is that $\sum_{n=k}^{\infty}\frac{1}{n}$ is a divergent series and so this proof attempt cannot be continued. Nonetheless Pólya suggests a possible reason for the failure. As the series $\sum_{n=1}^{\infty}a_i$ is assumed to be convergent, we know that a_i tends to 0 as i tends to infinity. Thus a_N will be much smaller than a_1 for large N. This has consequences for the Arithmetic-Geometric Mean Inequality. In particular, we know that the inequality is an equality if and only if the terms are all equal. Thus if the terms are unequal, the right hand side may be much larger than the left, leading to the introduction of the problematic divergent series.

Pólya's diagnosis suggest a way of fixing the attempt: make the terms of the sequence "more equal". A straightforward way of doing this is to consider multiplying each a_i by another factor c_i, to "balance out" the difference. Further "false starts" then help Pólya to come up with a suitable such sequence. In particular, the false starts reveal that we desire a sequence that is of the order of n and allows the sum $\sum_{n=k}^{\infty}\frac{1}{n(c_1c_2\ldots c_n)^{\frac{1}{n}}}$ to be evaluated.

As noted above, Sandborg found Pólya's reasons for adopting the auxiliary sequence strategy to be unsatisfying. He wrote:

> Thus, though he [Pólya] gave some indications that an auxiliary sequence would be helpful in giving a proof, he did not show that other approaches would be unpromising. We are left wondering if there might be another proof strategy that would succeed. It seems likely that Pólya's failure to address other proof strategies is part of the reason his motivations for using an auxiliary sequence appear somewhat vague, ill-defined, and unconvincing. Pólya showed that he has a promising strategy, but he did not show that it is more promising than other possibilities. (Sandborg, 1998, 145)

On my account, Pólya's first "false start" is more helpful. To analyze his motivational material in more detail, I will assume that the context contains elementary analysis and algebra, so that the reader is able to recognize the correctness of the proof steps. Additionally, I will assume that the Arithmetic-Geometric Mean Inequality is given a privileged status in the context so that it is easily accessible to the reader. However I will not assume that there are any special conventions or values in operation. Given this set up, Pólya's first false start should help the reader to uncover partial answers to the questions: "How does the c_i sequence advance the argument?" and "Where does it come from?"

More precisely, by showing the reader how the first proof attempt fails and how it can be fixed, Pólya's additional exposition helps the reader to grasp the role that the auxiliary sequence plays within the proof, "balancing out" the terms of the a_i sequence, and why this is important. At the same time, this reveals the nature of the connection between the c_i sequence and the Arithmetic-Geometric Mean Inequality. As this inequality has a privileged position within the context and clearly connects to the theorem in question, once its relationship to the c_i sequence is revealed the reader can, at least partially, describe where the sequence comes from.

As already mentioned, the first false start only provides partial answers to the questions of how the sequence advances the proof and where it comes from. However, Pólya's further false starts help the reader to provide more complete answers to these two questions, by identifying further roles that the sequence plays and their importance, and showing how these roles arise from modifications of plausible but inadequate attempts. Thus while Sandborg's account dismisses Pólya's reasoning about the first false start as "...somewhat vague, ill-defined, and unconvincing" (Sandborg, 1998, 145), my account takes it to be more valuable.

A further examination of Sandborg's account and my own reveals additional differences. First, Sandborg says that restrictions on what steps are appropriate can come from two places (Sandborg, 1998, 154): (a) previous steps in the proof; (b) the conclusion that is to be established. However, on my account, more must be taken into consideration because (recognizable) appropriateness is context dependent. For example, if certain values are in operation that restrict what resources may be appealed to, a step that invokes such forbidden resources will be neither contribution nor introduction appropriate. Further, even if all of

the steps are appropriate, if the proof has severe information management issues they may fail to be recognized as such. Finally, although Sandborg admits that "experience" may play a part in determining whether a proof step is arbitrary or not, he does not develop this further. My account, however, attempts to take this into consideration directly via the use of the context.

6.5 Concluding Remarks

In the above, I have suggested that my account of motivation is distinct from the theories of explanation developed by Kitcher and Steiner, and the theory of non-arbitrariness offered by Sandborg. More precisely, I suggested that there are proofs which meet the criteria of one account but not the other, assuming a suitable, but non-artificial context. Additionally, I argued that this was not just accidental, but occurred because the accounts are sensitive to different kinds of features. This provides strong evidence in support of my claim that the notion of motivation, as captured by my account, is something different from the notions of explanation and non-arbitrariness that are identified by the others. Further, as the notion of motivation that I have carved out has significant benefits (see section (4.5)), this suggests that it is worthy of investigation in its own right.

Some may still object that the accounts of explanation or non-arbitrariness that I have considered in this chapter are not "right" and once the "right" account has been discovered, it will subsume the notion of motivated proof that I have developed here. This may be true, but the burden of proof is on the proponent of the "right" account to develop it. Indeed, as mentioned in section (2.3.2), intuitions vary wildly about which proofs are explanatory and which are not, so such an account must be proposed before any such claim can be evaluated. Further, I am skeptical about such claims because it seems reasonable to suggest that there are multiple different ways in which a proof may be (or fail to be) explanatory or non-arbitrary. If this is correct, then it is important to identify these distinct senses and investigate them in their own right. Thus, even if someone argues that motivated proofs "really are" just explanatory proofs, there is still a need to analyze them.

Chapter 7

Conclusion

In drawing attention to proofs that are well motivated, mathematicians have highlighted a philosophically interesting virtue. Building on Pólya's work, I have offered an analysis of this virtue, carving out a more precise notion that, nonetheless, remains faithful to the guiding intuition that a reader wants to see that the steps in a proof are not just correct but also "appropriate". My account identifies two different senses of appropriateness and seeks to clarify them. Moreover, I develop the notion of a context to account for the fact that motivational efficacy (and appropriateness) is dependent on the "mathematical toolbox" that the reader has available to her. The context can be leveraged to better understand difficulties involved in the expansion and further development of mathematics. Indeed, our modern perspective can sometimes blind us to the subtleties involved in expanding mathematical tools and techniques, but considering the context, and paying attention to how the different components interact, can help us to better appreciate the difficulties that are involved. Finally, proofs that are motivated, according to my account, have a number of philosophically significant benefits, including increasing our understanding of how the proof works and the result itself, but also in helping the reader to more effectively use the ideas in her own work.

However, while I have carved out one precise class of motivated proofs, there may be others that are also of philosophical interest. Sandborg's account, which ties motivational efficacy to a lack of arbitrariness, is such a candidate. To be well motivated according to his account, a proof must meet conditions that are more stringent than the ones I suggest. While I maintain that there is an important sense in which proofs may be said to be well motivated

while containing steps that are, according to his account, somewhat arbitrary, this does not mean that his account should be rejected. Rather, both should be explored. Further, mathematicians often speak of proofs which are, for example, "geometrically motivated" (Sherali, 1987) or "physically motivated" (Halliwell, 2014). Proofs which are motivated in such a specific way may have additional benefits that other motivated proofs lack, and thus may be worth investigation in their own right.

Moreover, while I have focused on motivated *proofs* in this dissertation, other mathematical artifacts are often said to be motivated. For example, mathematicians call attention to definitions and theories which are (or fail to be) well motivated. Here are two examples:

> It is well known that not all algorithms are feasible; whether an algorithm is feasible or not depends on how many computational steps this algorithm requires. The problem with the existing definitions of feasibility is that they are rather *ad hoc*. Our goal is to use the maximum entropy (MaxEnt) approach and get more motivated definitions (Cooke et al., 1998, 25)

> Starting from a small number of well-motivated axioms, we derive a unique definition of sums with a noninteger number of addends. (Müller and Schleicher, 2011)

This suggests that it may be of philosophical interest to develop an account of motivational efficacy that applies to these artifacts as well. Indeed, there will likely be connections between the accounts themselves, as well as between accounts of other philosophically interesting virtues. For example, accounts of motivated definitions and theories may be closely related to accounts of fruitfulness, such as those proposed by Jamie Tappenden (Tappenden, 2008) and Audrey Yap (Yap, 2011). Finally, given the close connection between mathematics and science, the notions of motivated mathematical artifacts may generalize so as to apply to scientific concepts and theories.

Consequently the work undertaken in this dissertation is just the beginning of a philosophical investigation into motivational efficacy. However, it is not just philosophical work that remains to be done. As I suggested in the introduction, investigation into the topic of

motivated proofs, and motivated mathematical and scientific artifacts more generally, should be highly interdisciplinary.

Bibliography

G. Andrews. Letters to the editor. *The American Mathematical Monthly*, 97(3):215, March 1990.

G. Andrews. *Number Theory*. Courier Corporation, 2012.

G. Andrews and R. Baxter. A motivated proof of the Rogers-Ramanujan identities. *The American Mathematical Monthly*, 96(5):401–409, 1989.

J. Avigad. Understanding proofs. In Paolo Mancosu, editor, *The Philosophy of Mathematical Practice*. Oxford University Press, 2008. Page numbers are to the pre-print.

J. Avigad. Modularity in mathematics. In preparation, 201?

J. Avigad and R. Morris. Character and object. Manuscript in preparation.

J. Avigad and R. Morris. The concept of "character" in Dirichlet's theorem on primes in an arithmetic progression. *Archive for History of Exact Sciences*, 63(3):265–326, 2014.

A. Benjamin and J. Quinn. *Proofs that Really Count: The Art of Combinatorial Proof*. MAA, 2003.

Bernard Bolzano. *Wissenschaftslehre*. Sulzbach: Seidel, 1837.

H. Cohn. A short proof of the simple continued fraction expansion of e. *The American Mathematical Monthly*, 113(1):57–62, 2006.

D. E. Cooke, V. Kreinovich, and L. Longpr. Which Algorithms are Feasible? Maxent Approach. In G. Erickson, J. Rychert, and C. Smith, editors, *Maximum Entropy and*

Bayesian Methods, number 98 in Fundamental Theories of Physics, pages 25–33. Springer Netherlands, 1998.

K. Corrádi and S. Szabó. A generalized form of Hajós' theorem. *Communications in Algebra*, 21(11):4119–4125, 1993.

H. Davenport. *Multiplicative Number Theory*. Springer Science & Business Media, 2013.

C. de la Vallée Poussin. *Recherches analytiques sur la thorie des nombres premiers*. Hayez, 1897.

R. Dedekind. *Stetigkeit und irrationale Zahlen*. Vieweg: Braunschweig, 1872.

R. Dedekind. *Was sind und was sollen die Zahlen?* Vieweg: Braunschweig, 1888.

R. Dedekind. *Essays on the Theory of Numbers*. Merchant Books, 2008. Translated by W. Beman.

M. Detlefsen and A. Arana. Purity of methods. *Philosophers' Imprint*, 11(2), 2011.

L. Dickson. *History of the Theory of Numbers Volume 1: Divisibility and Primality*. Courier Dover Publications, 2012.

J. Dirichlet. Sur la convergence des séries trigonométriques qui servent à représenter une fonction arbitraire entre des limites données. *Journal für die reine und angewandte Mathematik*, pages 157–169, 1829. Reprinted in Dirichlet (1989), pages 117–132. Page numbers given in the references are to the reprint.

J. Dirichlet. 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*, pages 45–81, 1837a. Reprinted in Dirichlet (1989), pages 313–342. Translated by Ralf Stefan as "There are infinitely many prime numbers in all arithmetic progressions with first term and difference coprime," arxiv:0808.1408. Page numbers given in the references are to the English translation.

J. Dirichlet. Beweis eines Satzes über die arithmetische Progression. *Bericht über die Verhandlungen der königlich Presussischen Akademie der Wissenschaften Berlin*, 1837b. Reprinted in Dirichlet (1989), pages 307–312. Page numbers given in the references are to the reprint.

J. Dirichlet. Untersuchungen über die Theorie der complexen Zahlen. *Abhandlungen der Königlich Preussischen Akademie der Wissenschaften von 1841*, 19/21, 1841. Reprinted in (Dirichlet, 1989), pages 509-532. Page numbers given in the references are to the reprint.

J. Dirichlet. *Werke*. G. Reimer, 1989. edited by L. Kronecker.

P. Erdős, J. Suranyi, and B. Guiduli. *Topics in the Theory of Numbers*. Springer New York, 2003.

L. Euler. Theorematum quorundam ad numeros primos spectantium demonstratio. *Commentarii academiae scientiarum Petropolitanae*, 8 (1736), 1741. Available online, along with an English translation, at `http://eulerarchive.maa.org/`.

L. Euler. Theoremata circa divisores numerorum. *Novi Commentarii academiae scientiarum Petropolitanae*, (1):20–48, 1750. English translation by D. Zhao available at the Euler Archive http://eulerarchive.maa.org. Page references are to the translation.

G. Everest and T. Ward. *An Introduction to Number Theory*. Springer Science and Business Media, 2006.

J. Frans and E. Weber. Mechanistic explanation and explanatory proofs in mathematics. *Philosophia Mathematica*, 22:231–248, 2014.

R. Friedberg. *An Adventurer's Guide to Number Theory*. Dover Publications, 1995.

J. Hafner and P. Mancosu. The Varieties of Mathematical Explanation. In P. Mancous, K. Jrgensen, and S. Pedersen, editors, *Visualization, Explanation and Reasoning Styles in Mathematics*, pages 215–250. Springer Netherlands, 2005.

J. Hafner and P. Mancosu. Beyond Unification. In P. Mancosu, editor, *The Philosophy of Mathematical Practice*, pages 151–178. Oxford University Press, 2008a.

Johannes Hafner and Paolo Mancosu. Beyond Unification. In Paolo Mancosu, editor, *The Philosophy of Mathematical Practice*, pages 151–178. Oxford University Press, June 2008b. ISBN 9780199296453. URL http://www.oxfordscholarship.com/view/10.1093/acprof:oso/9780199296453.001.0001/acprof-9780199296453-chapter-7.

J. Halliwell. Two proofs of Fine's theorem. *Physics Letters A*, 378(40):2945–2950, August 2014.

H. Hastings. Mathscinet review MR0563240 (81c:55026), 1981.

D. Hilbert. *The Theory of Algebraic Number Fields*. Springer Science & Business Media, 1998. Translated by I. Adamson. With an introduction by F. Lemmermeyer and N. Schappacher.

J. Ivory. Demonstration of a theorem respecting prime numbers. In T. Leybourn, editor, *New series of The mathematical repository*, pages 6–8. W. Gledinning, 1806.

T. Jones. Discovering and proving that π is irrational. *The American Mathematical Monthly*, 117(6):553–557, 2010.

P. Kitcher. Explanatory unification and the causal structure of the world. In P. Kitcher and W. Salmon, editors, *Scientific Explanation*, volume 8, pages 410–505. Minneapolis: University of Minnesota Press, 1989.

L. Kronecker and K. Hensel. *Vorlesungen über Zahlentheorie*. B.G. Teubner, 1901.

J. Lagrange. Demonstration d'un théorème nouveau concernant les nombres premiers. *Nouveaux Mémoires de l'Académie Royale des Sciences et Belles-Lettres (Berlin)*, 2:125–137, 1773. Reprinted in (Serret and Darboux, 1869, 425–438).

M. Lange. Why proofs by mathematical induction are generally not explanatory. *Analysis*, 69:203–211, 2009.

J. Loxton. Mathscinet review MR0702190 (85h:11041), 1985.

R Morris. Character and object. Master's thesis, Carnegie Mellon University, 2011.

M. Müller and D. Schleicher. How to add a noninteger number of terms: from axioms to new identities. *American Mathematical Monthly*, 118(2):136–152, 2011.

Papercuts. Prove every odd integer is the difference of two squares. Mathematics Stack Exchange. URL `http://math.stackexchange.com/q/263101`. URL:http://math.stackexchange.com/q/263101 (version: 2012-12-21).

G. Pólya. With, or without, motivation. *The American Mathematical Monthly*, 56(10): 684–691, 1949.

M. Resnik and D. Kushner. Explanation, Independence and Realism in Mathematics. *The British Journal for the Philosophy of Science*, 38(2):141–158, June 1987.

C. A. Rogers. Lusin's second separation theorem. *Journal of the London Mathematical Society*, s2-6(3):491–503, May 1973.

D. Sandborg. *Explanation in Mathematical Practice*. PhD thesis, Department of History and Philosophy of Science, University of Pittsburgh, 1998.

J. Serret and G. Darboux, editors. *Oeuvres de Lagrange*. Gauthier-Villars, 1869.

H. Sherali. A Constructive Proof of the Representation Theorem for Polyhedral Sets Based on Fundamental Definitions. *American Journal of Mathematical and Management Sciences*, 7(3-4):253–270, February 1987.

W. Sieg. Searching for proofs (and uncovering capacities of the mathematical mind). In *Hilbert's Programs and Beyond*, pages 377–401. Oxford University Press, 2013.

E. Stein and R. Shakarchi. *Fourier Analysis: An Introduction*. Princeton University Press, 2011.

M. Steiner. Mathematical explanation. *Philosophical Studies*, 34(2):135–151, 1978.

J. Stillwell. *Lectures on Number Theory, P.G.L. Dirichlet with supplements by R. Dedekind*. American Mathematical Society, 1999.

J. Tappenden. Mathematical concepts: Fruitfulness and naturalness. In Paolo Mancosu, editor, *The Philosophy of Mathematical Practice*. Oxford University Press, 2008.

J. Toeplitz. Der Fermat'sche und der Wilson'sche Satz, einer gemeinschaftlichen Quelle abgeleitet. *Archiv der Mathematik und Physik*, 32:104–106, 1859.

Wick. Proof that every odd integer is a difference of two squares. Mathematics Stack Exchange. URL `http://math.stackexchange.com/q/510096`. URL:http://math.stackexchange.com/q/510096 (version: 2013-09-30).

A. Yap. Gauss' quadratic reciprocity theorem and mathematical fruitfulness. *Studies in History and Philosophy of Science Part A*, 42(3):410–415, 2011.