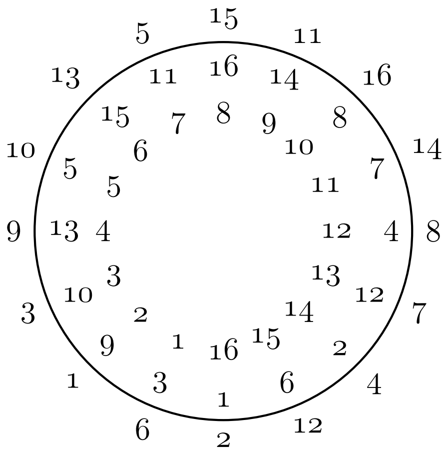
Discrete Logarithms

Mathematics and Art

David Pierce

December 17, 2017–August 13, 2020
Matematics Department
Mimar Sinan Fine Arts University, Istanbul
mat.msgsu.edu.tr/~dpierce/
polytropy.com



Contents

List of Tables

List of Figures

Introduction

The core of this document is the two tables, of logarithms and antilogarithms respectively, constituting Chapter 2. The numbers in the tables may appear to be random. However, you can check in specific cases that each table undoes the other: for example, since the first table gives 564 as the logarithm of 319, the second table inevitably gives 319 as the antilogarithm of 564. The antilogarithm of 1 is 7, and each successive antilogarithm is either 7 times the previous, or else it is the remainder of that multiple after division by 997. Therefore the logarithms can be used as Briggsian or common logarithms once were, for computing products by taking sums. The logarithm of the product is the sum of the logarithms, though sums now are taken *modulo* 996, and products *modulo* 997.

In the terminology of Euler, 7 is a *primitive root* of 997. Chapter 3 reviews the mathematics, from Euclid to Gauss and beyond. If sufficiently interested, the layperson may follow the review, while the professional may still find something new.

Anyone may contemplate the tables as conceptual art. I consider art as such in Chapter 1, mainly through the work of R. G. Collingwood, but also Mary Midgley, Arthur Danto, and others. I review other examples of conceptual art.

I quote theory and scholarship, poetry and fiction, mostly from books in my personal collection. The quotations may be considered as if they were readymades of Marcel Duchamp, or pictures in the exhibition that I am curating.

1 Art

1.1 Creation

What counts as art today is broader than Collingwood contemplated in 1938 in *The Principles of Art* [11]. Nonetheless, the book remains invaluable.

In writing poems, or painting pictures, or composing quartets, or even—I would add—proving mathematical theorems, before you can employ a *technique,* according to a *plan,* you have to discover how to do everything in the first place. This need seems easily overlooked. Collingwood points it out. In creating your work of art, you cannot say—you cannot *express*—in any precise way, what you are trying to do, before figuring out how to it. The figuring out is precisely the expressing of it.

Expression is the key word. As Collingwood says on his page 151,

> By creating for ourselves an imaginary experience or activity, we express our emotions; and this is what we call art.

This is not a conclusion, but a halfway point; the text will end on page 336. It is important to read further, here into page 152:

> What this formula means, we do not yet know. We can annotate it word by word; but only to forestall misunderstandings, thus. 'Creating' refers to a productive activity which is

> not technical in character. 'For ourselves' does not exclude 'for others'; on the contrary, it seems to include that; at any rate in principle. 'Imaginary' does not mean anything in the least like 'make-believe', nor does it imply that what goes by that name is private to the person who imagines. The 'experience or activity' seems not to be sensuous, and not to be in any way specialized: it is some kind of general activity in which the whole self is involved. 'Expressing' emotions is certainly not the same thing as arousing them. There is emotion there before we express it . . .

We are faced now with three problems: to understand (1) imagination, (2) emotion, and (3) their connection.

> These problems must be dealt with . . . not by continuing to concentrate our attention on the special characteristics of aesthetic experience, but by broadening our view, so far as we can, until it covers the general characteristics of experience as a whole.

I propose to consider this broadened view as encompassing mathematics.

I say that art and mathematics are creations. You may disagree. In *Heart and Mind* from 1981, in the chapter called "Creation and Originality," Mary Midgley takes issue with the treatment of creation by Collingwood and others, especially Nietzsche and Sartre [46, pp. 49–67]. She begins with the importance of her subject, which is morality rather than art as such.

> The creation of moral values is a pressing topic because, whether we use words like *creation* or not, we all need to find new moral ideas to help us deal with a confused and changing world. The notion that these ideas must be totally new, that they should not rest at all on traditional supports, exists and concerns us all.

The God of Genesis calls light into existence and *then* sees that it is good [7]. God causes dry land to appear and *then* sees it as good. Likewise with grass, herb, and tree, and with the lights of heaven, and so forth: first they are created, and then they are evaluated. Not even God just *declares* what is good: its existence is by fiat, but not its goodness.

As for ourselves, if we are no longer going to take our values from heaven, there is no sense in trying to do what not even its mythical ruler can do. This is what I understand Midgley to argue. "If God is really dead," she says, "why should we dress up in his clothes?" We cannot just will things into existence, especially not goodness:

> The human will is not a mechanism for generating new thoughts out of nothing. It is a humble device for holding onto the thoughts which we have got and using them.

The will then is not creative, but preservative. It may thus be humble, but it is still essential. Students need it, especially when they carry around the little electronic devices that are designed to draw their attention—to draw and quarter it, one might say. The student needs attention, application, *persistence,* as I observed elsewhere [53, p. 245]. As expressing the thought, I quoted one of William Blake's "Proverbs of Hell" from *The Marriage of Heaven and Hell* [4, plate 7]:

> If the fool would persist in his folly he would become wise.

That the creativity of civilization depends on persistence is an argument for the *rise* of what Julian Jaynes calls the bicameral mind, although the title of his 1976 book is *The Origin of Consciousness in the Breakdown of the Bicameral Mind.* Other animals go about their business naturally, but civilization is an unnatural business. It requires us, in youth and later, to do things that we do not see the point of. The *will* to do these things has needed to evolve. For Jaynes, one stage in this evolution was the hearing of voices that kept us at work. "Let us consider a man," he says [36, pp. 134 f.],

> commanded by himself or his chief to set up a fish weir far upstream from a campsite. If he is not conscious, and cannot therefore narratize the situation and so hold his analog 'I' in a spatialized time with its consequences fully imagined, how does he do it? It is only language, I think, that can keep him at this time-consuming all-afternoon work. A Middle Pleistocene man would forget what he was doing. But lingual man would have language to remind him, either repeated by himself, which would require a type of volition which I do not think he was then capable of, or, as seems more likely, by a repeated 'internal' verbal hallucination telling him what to do . . . learned activities with no consummatory closure do need to be maintained by something outside of themselves. This is what verbal hallucinations would supply.

How we have come to be where we are is indeed a puzzle, though I shall not dwell on Jaynes's attempt at a solution. We can think of the puzzle both on a "special" scale—the scale of our species—and on a personal scale, as Collingwood does in his last book, from 1942, *The New Leviathan: Or Man, Society, Civilization, and Barbarism.* Here Collingwood takes issue with the notion of Rousseau that "Man is born free, and everywhere he is in chains."

"I do not doubt," says Collingwood [13, p. 176], "that truths, and important truths, can be told in Rousseau's language." However,

> **23. 93.** In human infancy the fact, as known to me at least, is that a man is born neither free nor in chains.
>
> **23. 94.** To be free is to have a will unhampered by external force, and a baby has none.

> **23. 95.** To be in chains is to have a will hampered by something which prevents it from expressing itself in action; and a baby has none.
>
> **23. 96.** A man is born a red and wrinkled lump of flesh having no will of its own at all, absolutely at the mercy of the parents by whose conspiracy he has been brought into existence.
>
> **23. 97.** That is what no science of human community, social or non-social, must ever forget.

I wonder whether Midgley forgets these facts in *Heart and Mind.* She does recognize that creation can be perceived on a smaller scale than Genesis. Indeed, she quotes Collingwood from *The Principles of Art* as showing this. Here he is, in an expansion of Midgley's quotation [11, pp. 128 f.].

> Readers suffering from theophobia will certainly by now have taken offence . . . Perhaps some day, with an eye on the Athanasian Creed, they will pluck up courage to excommunicate an arithmetician who uses the word three. Meanwhile, readers willing to understand words instead of shying at them will recollect that the word 'create' is daily used in contexts that offer no valid ground for a fit of *odium theologicum* . . .
>
> To create something means to make it non-technically, but yet consciously and voluntarily. Originally, *creare* means to generate, or make offspring, for which we still use its compound 'procreate' . . . The act of procreation is a voluntary act, and those who do it are responsible for what they are doing; but it is not done by any specialized form of skill . . . It is in this sense that we speak of creating a disturbance or a demand or a political system. The person who makes these things is acting voluntarily; he is acting responsibly; but he need not be acting in order to achieve any ulterior end; he need not be following a preconceived plan; and he

> is certainly not transforming anything that can properly be called a raw material. It is in the same sense that Christians asserted, and neo-Platonists denied, that God created the world.

Midgley objects, in a way that suggests to me that she has not really thought about what it means to grow up, or even what it means to compose an essay such as her own.

1.2 Gender

Midgley's experience of writing and life is no doubt different from mine. An important difference is connected to the English gendered pronouns. Our *first*-person pronouns are epicene; but in the third person, I become he, while Midgley is she.

The distinction is not imposed on us by nature. Each of us, including objects thought to be inanimate, is simply *o* in Turkish, which is a language "born free" of "the curse of grammatical gender" [41, II.26, p. 48]. In English, we have a vestige of the curse, a vestige that can either reflect differences in experience, or *effect* them.

In 2013, Midgley wrote to *The Guardian* as follows [47]. She was responding to the question of "why, though five quite well-known female philosophers emerged from Oxford soon after the war, few new ones are doing so today."

> As a survivor from the wartime group, I can only say: sorry, but the reason was indeed that there were fewer men about then. The trouble is not, of course, men as such—men have done good enough philosophy in the past. What is wrong is a particular style of philosophising that results from encouraging a lot of clever young men to compete in

> winning arguments. These people then quickly build up a set of games out of simple oppositions and elaborate them until, in the end, nobody else can see what they are talking about. All this can go on until somebody from outside the circle finally explodes it . . . By contrast, in those wartime classes—which were small—men (conscientious objectors etc) were present as well as women, but they weren't keen on arguing.
>
> It was clear that we were all more interested in understanding this deeply puzzling world than in putting each other down. That was how Elizabeth Anscombe, Philippa Foot, Iris Murdoch, Mary Warnock and I, in our various ways, all came to think out alternatives to the brash, unreal style of philosophising—based essentially on logical positivism—that was current at the time.

It is unfortunate that war had to create an opportunity, both for women to pursue and develop their thoughts, and for men to learn from them, as I have learned from Midgley. In *Evolution As a Religion,* she rightfully critiques the presumption of some scientists (generally male) in making grand pronouncements on the meaning of life from physical theories. She quotes Steven Weinberg as saying, in an "excellent and informative little book,"

> The more the universe seems comprehensible, the more it also seems pointless.
>
> But . . . The effort to understand the universe is one of the very few things that lifts [*sic*] human life a little above the level of farce, and gives it some of the grace of tragedy.

Midgley observes [45, p. 87],

> Since virtually the whole book has been devoted to expounding astrophysics, not to discussing it as an occupation, and certainly not to discussing other occupations with which it

> might compete, Weinberg's readers might find this an unexpected blow. They might feel rather shaken and degraded by the sudden revelation that their lives are probably valueless, and they might also ask the reasonable question: how does Weinberg know?

Obviously Weinberg is only giving his opinion. The problem is not the rudeness of stating such an opinion, but the unscientific practice of deriving the opinion *from* science, rather than recognizing it as connected with why one has done science in the first place.

Here I may have passed to my own thought, only prompted by Midgley. Our subject was art and creation, and I still wonder whether Midgley has understood Collingwood when she says [46, pp. 64 f.],

> It may seem that at this point the word 'create' has been diluted into complete triviality, that it simply means 'make'. But it still keeps an awkward core of special meaning, and one that is important for Collingwood's theory of art. On his view, creators need not, indeed characteristically do not, know in advance what they are going to make. He sees the absence of a 'preconceived end' as a mark of real art, a mark which distinguishes it from mere craft. But if you really do not know what you are trying to bring about, it is hard to see how you can do it, and harder still to see how you can be called responsible. Artists don't in fact often talk in this way. They are often quite willing to discuss their aims and problems. But whether or not sense can be made of this for art, in morals it is surely a non-starter.

This shows the difficulty of understanding Collingwood. He does indeed distinguish art from craft; but there is no X-ray machine that you can feed artefacts into, and a light flashes green for art, red for craft. The same object has aspects of both. It is not even the *physical* object that can be a work of art at all. We shall come back to this later, on page 25.

After taking an examination, students want to know how they did. If they do not already know this, just from what they themselves have written on their papers, then they must not have had a preconceived end in any precise sense. They want a good grade, but they do not know what this really means. If they have done well, according to their teacher, they may still be proud, and they have some right to be, since they are responsible for what they did.

I had an aim when I set out to write this essay. I could have talked about the aim in general terms. But the aim has grown, and grown precise, just as the essay has taken shape. In particular, at the beginning, I had no idea of the current sectional divisions of this essay.

1.3 Individualism

This essay is an *expression.* The term was key for art of Collingwood's time, notably that of the *Blaue Rieter* group, formed in Munich by Franz Marc in 1911. According to Herbert Read in *A Concise History of Modern Painting* [60, p. 228],

> *Blaue Reiter* was the first coherent attempt to show that what matters in art—what gives art its vitality and effect—is not some principle of composition or some ideal of perfection, but a direct expression of feeling, the form corresponding to the feeling, as spontaneous as a gesture, but as enduring as a rock.

Read begins his book with a long quotation from Collingwood's 1924 book, *Speculum Mentis or The Map of Knowledge.* The idea is that, "in art, a school once established normally deteriorates as it goes on" [10, p. 82]. Collingwood's ideas themselves continued to develop. He published *Outlines of a Philosophy of Art* in 1925, but updated his views a dozen years later in *The Principles of Art.* Concerning the quotation that Read makes, but does not really analyze, from *Speculum Mentis,* I suggest that a school of art, once founded, declines, precisely because its very foundation constitutes the identification of a technique, and technique is not art.

In its article on Aesthetics, the *Internet Encyclopedia of Philosophy* [63] is misleading to suggest that Collingwood "took art to be a matter of self-expression." There was no need to add the restriction to the self. This assertion in the *Encyclopedia* is indeed followed by the formula from *The Principles of Art* quoted above, whereby art is a creating for our *selves.* However, if one reads beyond the formula, also as above, then one sees how Collingwood was at pains to keep references to the self from being misunderstood. Creating art for ourselves includes doing it for others. One's imagination need not be private to oneself.

The central lesson of *mathematics* is that each of us has the right to decide, for her- or himself, what is true. Mathematical truth does not come down from heaven, but comes up from within each of us. It is like art in this way.

Mathematical truth is nonetheless common. In mathematics, we have the responsibility of resolving disputes amicably, because anything on which there is fundamental disagreement is not mathematics.

It may not be art either.

What is *liked* may differ from person to person, whether we are talking about art or mathematics. Some mathematicians do not like the method of proof by contradiction. They should still agree on whether a given proof by contradiction is *correct* as a proof by contradiction. Likewise should we all be able to agree on whether something is art; but the truth of this assertion is not so clear as the corresponding one for mathematics. This is a *practical* reason why everybody should learn some mathematics: it teaches the possibility, if not the obligation, of peaceful resolution of differences.

The theme that what is *mental* need not be merely *personal* goes back to Collingwood's first book, *Religion and Philosophy* of 1916 [9, p. 93]. In the chapter called "Matter," concerning this as distinguished from mind, Collingwood wrote,

> A boot is more adequately described in terms of mind—by saying who made it and what he made it for—than in terms of matter. And in the case of all realities alike, it seems that the materialistic insistence on their objectivity is too strong; for it is not true that we are unable to alter or create facts, or even that we cannot affect the course of purely "inanimate" nature. Materialism, in short, is right as against those theories which make the world an illusion or a dream of my own individual mind; but while it is right to insist on objectivity, it goes too far in describing the objective world not only as something different from, and incapable of being created or destroyed by, my own mind, but as something different and aloof from mind in general.

Again, though art be expression, it is not *self*-expression as such.

In *The Principles of Art,* even before formulating the tentative definition of art that we have seen, Collingwood argues that art is not merely a private concern. Art is for the world, for civilization, even though civilization may not respect this [11, pp. 33 f.]:

> Here lies the peculiar tragedy of the artist's position in the modern world. He is heir to a tradition from which he has learnt what art should be; or at least, what it cannot be. He has heard its call and devoted himself to its service. And then, when the time comes for him to demand of society that it should support him in return for his devotion to a purpose which, after all, is not his private purpose but one among the purposes of modern civilization, he finds that his living is guaranteed only on condition that he renounces [*sic*] his calling and uses [*sic*] the art which he has acquired in a way which negates its fundamental nature, by turning journalist or advertisement artist or the like; a degradation far more frightful than the prostitution or enslavement of the mere body.

It *is* disappointing that, in closing this passage, Collingwood takes up the mind-body dualism that he refuted in *Religion and Philosophy.* One might say, echoing him there, "Prostitution is more adequately described in terms of mind—by saying it compromises one's capacity to love and be loved—than in terms of matter."

Collingwood reiterates the universality of art at the end of *The Principles of Art* [11, p. 333], where he observes first (writing before 1938) that English painting and literature aim no longer just to amuse the wealthy, but to be competent as art.

> But the question is whether this ideal of artistic competence is directed backwards into the blind alley of nineteenth-century individualism, where the artist's only purpose was to express himself, or forwards into a new path where the

> artist, laying aside his individualistic pretensions, walks as the spokesman of his audience.
>
> In literature, those who chiefly matter have made the choice, and made it rightly. The credit for this belongs in the main to one great poet, who has set the example by taking as his theme in a long series of poems a subject that interests every one, the decay of our civilization.

The poet is T. S. Eliot. Collingwood's conclusion is preceded by theory. After the formula for art from his page 151 quoted earlier, in starting to develop a theory of the imagination, Collingwood distinguishes thought from feeling. One distinction is that while feelings are private, thoughts are potentially public, or held in common [11, p. 157]. One's own feeling of cold has no relation to anybody else's; but the thought that a house is ten degrees Celsius is the same for everybody in the house who has the thought.

1.4 Eros

By bringing feelings into consciousness, art allows them to be shared. Art is ultimately identified with *language.* This is not language as a system for communication: developing such a system requires language in the first place.

We are talking about language such as Archimedes uttered, when he exclaimed "Eureka!" in the story told by Vitruvius [65, pp. 36 f.]. The expression of the mathematician was not just the first-person singular perfect form *εὕρηκα* of the verb *εὑρίσκω* "find"; it was the cry of a thinker who had just understood how to test the golden crown of King Hiero for adulteration with silver. "And if there had been among the passers-by," suggests Collingwood [11, p. 267],

> a physicist as great as Archimedes himself, who had come to Syracuse in order to tell Archimedes that he had discovered specific gravity, it is not impossible that he might have understood the whole thing, and burst from the crowd, shouting, 'So have I!'

Collingwood admits that the imaginary example involving Archimedes is "extreme and fantastic." So is John Donne's argument about language and perception in his poem "The Extasie" (of the early seventeenth century), comprising 76 lines [18, pp. 39–41]. Donne and his beloved sit all day, holding hands, staring into one another's eyes, "Our eye-beams twisted":

> If any, so by love refin'd,
> That he soules language understood,
> And by good love were growen all minde,
> Within convenient distance stood,
> He (though he knew not which soul spake,
> Because both meant, both spake the same)
> Might thence a new concoction take,
> And part farre purer than he came.

The refined soul speaks the language in which the love of the chaste couple is expressed; but many souls are not so refined, and so, for *their* sake, the couple ought to be more physically entwined.

> To'our bodies turne we then, that so
> Weake men on love reveal'd may looke;
> Loves mysteries in soules doe grow,
> But yet the body is his booke.
> And if some lover, such as wee,
> Have heard this dialogue of one,
> Let him still marke us, he shall see
> Small change, when we'are to bodies gone.

Let me suggest in passing that, if a man today really does fear to approach a woman, lest he be accused of harrassment, then let him try writing a poem like Donne's. It may not get him what he wants, but he may learn something else.

Language may be used for *self*-expression, but this was not any more commendable for Collingwood than it was for E. B. White, who wrote in his contribution to *The Elements of Style* in the 1950s [70, p. 59],

> The volume of writing is enormous, these days, and much of it has a sort of windiness about it, almost as though the author were in a state of euphoria. "Spontaneous me," sang Whitman, and in his innocence let loose the hordes of uninspired scribblers who would one day confuse spontaneity with genius.

I do not know whether White meant to allude to the erotic *content* of Whitman's actual poem. Any poem is a list of lines; most of the 45 lines of "Spontaneous Me" [69, pp. 89–91] are longer than an ordinary printed page is wide, and most of them are noun phrases, or series of noun phrases, serving as the subject, or rather as an appositive to the subject, of one long sentence, whose verb does not come till the last line:

> Spontaneous me, Nature,
> The loving day, the mounting sun, the friend I am happy with,
> The arm of my friend hanging idly over my shoulder,
> The hillside whiten'd with blossoms of the mountain ash,
> The same late in autumn, the hues of red, yellow, drab, purple, and light and dark green,
> . . . .

> The consequent meanness of me should I skulk or find myself indecent, while birds and animals never once skulk or find themselves indecent,
> The great chastity of paternity to match the great chastity of maternity,
> The oath of procreation I have sworn, my Adamic and fresh daughters,
> The greed that eats me day and night with hungry gnaw, till I saturate what shall produce boys to fill my place when I am through,
> The wholesome relief, repose, content,
> And this bunch pluck'd at random from myself,
> It has done its work—I toss it carelessly to fall where it may.

The ellipsis stands for lines that are likewise interesting and graphic in themselves, but that go on and on, with a logic that may be as obscure as the logic of the list of logarithms excerpted below in Table 1.4 (page 39) and given subsequently in full in Chapter 2.

1.5 Analysis

I used *Religion and Philosophy* to illustrate *The Principles of Art.* I think one can do this, even though Collingwood disavowed the earlier book, soon after publication. Around 1918, he added the following remarks to the proofs, which he had saved and bound [14, pp. xxii f.]:

> This book was written in (and before) 1914 (begun 1912) and represents the high-water mark of my earliest line of thought—dogmatic belief in New Realism in spite of an insight into its difficulties which I think none of my teachers

> shared . . . The whole thing represents a point of view I should entirely repudiate, and its complete failure with the public gives me great satisfaction.

The "new realists" were apparently the early exponents of so-called analytic philosophy. I wonder if Collingwood isn't little known today, precisely because of his distancing of himself from what became analytic philosophy.

Stephen Trombley describes the general situation in *Fifty Thinkers Who Shaped the Modern World.* Unfortunately the book has but a single bibliography, and no notes, and so Trombley's sources are not clear; neither is there an index, but Trombley seems not to name Collingwood. Nonetheless, some of what Collingwood has to say in his 1939 autography is reflected in Trombley's chapter on F. H. Bradley [66, p. 115]:

> In the period between 1850 and 1903 there wasn't a school of British *idealism,* there was simply *British* philosophy, the general tendency of which was idealist. 'British idealism' is better regarded as a pejorative term created by early analytic philosophers to identify the status quo they wished to supplant with their own brand of thinking. The strange death of idealism in British philosophy goes hand in hand with philosophy's transformation from a gentleman's pastime into a profession . . . [T. H.] Green's career is a milestone in the history of philosophy because, according to the utilitarian Henry Sidgwick (1838–1900), he was the first *professional* philosopher in the English-speaking world.
>
> The early analytic philosophers' war on British idealism can be seen to involve much more than the desire to supplant neo-Hegelian idealism and metaphysics in its entirety with logicism: they also wanted the idealists' jobs. The analytic side won both battles. The professionalization of philosophy in Britain and the United States resulted in the death

> of idealism and the erection of analytic philosophy as the official way of thinking; in this way a generation of teachers led by Russell, Moore and Wittgenstein spawned a new generation of followers, who in turn kept the analytic torch burning brightly in the English-speaking world throughout the twentieth century as their students and their students' students took up university teaching jobs. (There are notable exceptions . . .)

In *An Autobiography* [12], Collingwood admires what he calls the school of Green. Those who charted a different course from Green's, by devaluing thought, by teaching such doctrines as Cook Wilson's "knowing makes no difference to what is known": they laid the ground for British support of Spanish fascism and German Nazism, at least as of November 2, 1938, the date of the Preface of *An Autobiography.* (The Munich agreement was signed on September 29 of that year [37, p. 250].)

In *What Art Is* of 2013, Arthur Danto considers art that Collingwood did not live to see. However, Danto works in the analytic tradition quite literally, dividing up philosophy into components of ontology and epistemology [15, p. 5].

> When they see work that puzzles them, people ask, "But is it art?" At this point I have to say that there is a difference between *being* art and knowing whether something *is* art. Ontology is the study of what it means to be something. But knowing whether something is art belongs to epistemology—the theory of knowledge—though in the study of art it is called connoisseurship. This book is intended mostly to contribute to the ontology of Art, capitalizing the term that it applies to widely—really to everything that members of the art world deem worthy of being shown and studied in the great encyclopedic museums.

The encyclopedic museums are such as the Metropolitan in New York or the National Gallery in Washington, as Danto has said on the previous page.

1.6 Concepts

What then is art? Danto wants a *definition.* He is not satisfied with the idea from Wittgenstein that works of art need share only a family resemblance [15, pp. 29–34]. Neither does Danto seem to like the idea of the "open concept," attributed to Morris Weitz in 1956. The Institutional Theory of art developed by George Dickie in the 1960s is inadequate since, in Danto's example, the head of the National Museums of Canada, despite his leading position in the Art World, was able to be wrong in denying artistic status to those peculiar works, discussed below, called *readymades.*

We might show further the inadequacy of the Institutional Theory by observing that poems and music can be art, but are not the kind of thing that is displayed in a museum. Of course they may be given official status in other ways. However, despite or because of this official status, a national anthem, or the output of a poet laureate, is not art; it is the kind of craft called *magic* in *The Principles of Art.* We shall return to this on page 27. Meanwhile, even though Danto uses the term *art* to mean *visual* art, implicitly excluding poetry and music, his theme is that what makes something art is invisible.

Key works for Danto's considerations are (1) Marcel Duchamp's 1915 readymade called *In Advance of the Broken Arm,* which was a snow shovel from a hardware store on Columbus Avenue in New York, and (2) Andy Warhol's *Brillo Box,* or boxes, of the 1960s. How can these be art, when they look just like things that are not art? For Danto [15, p. 37],

> My sense is that, if there were no visible differences, there had to have been *invisible differences*—not invisible like the Brillo pads packed in the Brillo boxes [but not in Warhol's boxes], but properties that were *always* invisible. I've proposed two such properties that are invisible in their nature. In my first book on the philosophy of art I thought that works of art are *about* something, and I decided that works of art accordingly have meaning. We infer meanings, or grasp meanings, but meanings are not at all material. I then thought that, unlike sentences with subjects and predicates, the meanings are *embodied* in the object that had them. I then declared that works of art are *embodied meanings.*

As far as I can tell, meaning is *one* of the two invisible properties that Danto has proposed for the work of art. The other property is being a waking dream [15, p. 48]:

> I have decided to enrich my earlier definition of art—embodied meaning—with another condition that captures the skill of the artist. Thanks to Descartes and Plato, I will define art as "wakeful dreams."

Danto has turned to Plato and Descartes—to the *Meditations* of the latter and the Divided Line in the *Republic* of the former—because they deal with the distinction between dreaming and perceiving, and this is like the distinction between Warhol's Brillo boxes and the real thing.

We all have to make our own way in the world. In his 1991 philosophical novel *Lila* [56, ch. 26, pp. 370–2], Robert Pirsig coins a useful word, defined by an analogy:

> Philosophology is to philosophy as musicology is to music, or as art history and art appreciation are to art, or as literary criticism is to creative writing.

One might add two more terms to the analogy: history and philosophy of mathematics, and mathematics itself. According to Pirsig, "philosophologists" put

> a philosophological cart before the philosophical horse. Philosophologists not only start by putting the cart first; they usually forget the horse entirely. They say first you should read what all the great philosophers of history have said and *then* you should decide what *you* want to say. The catch here is that by the time you've read what all the great philosophers of history have said you'll be at least two hundred years old.

You have to do your own work. It still seems to me that Arthur Danto might have saved himself some trouble by reading a philosopher of art from the previous generation. If a work of art is an *expression,* as Collingwood observes, then it is simply not a physical object. In particular, it should not be expected to have *properties* of physical objects. Perhaps Danto need not have spent years figuring this out again.

Collingwood's ultimate expression of the idea is in the first two chapters of his last book, quoted earlier, namely *The New Leviathan.* We are not made up of two parts, called body and mind. We rather have two ways of thinking. In their most refined forms, these ways can be called, respectively, (1) sciences of nature, physical sciences, or sciences of body, and (2) sciences of mind. Here is Collingwood [13, pp. 7–11].

> **1. 83.** Man as body is *whatever the sciences of body say that he is.* Without their help nothing can be known on that subject: their authority, therefore, is absolute.
>
> **1. 84.** Man as mind is *whatever he is conscious of being.*
>
> . . . .

> **2. 43.** For man's body and man's mind are not two different things. They are one and the same thing, man himself, as known in two different ways.
>
> **2. 44.** Not a part of man, but the whole of man, is body in so far as he approaches the problem of self-knowledge by the methods of natural science.
>
> **2. 45.** Not a part of man, but the whole of man, is mind in so far as he approaches the problem of self-knowledge by expanding and clarifying the data of reflection.
>
> . . . .
>
> **2. 48 . . .** In the natural sciences, mind is not that which is left over when explaining has broken down; it is what does the explaining . . .

Sciences of mind are *criteriological* sciences, like logic, ethics, history, economics. They study whether something—some instance of *thinking*—is going well or ill. How this thinking is proceeding is judged not only by an external standard (in which case, for its study, the term *normative science* might be sufficient); it is judged by the standards or *criteria* of the thinking itself.

Collingwood introduces the term *criteriological* in a note in *The Principles of Art* [11, p. 171], though the concept itself is found in *An Essay on Philosophical Method* of 1933. In this *Essay* is also found the reason why it is hard to stick with one subject when thinking about Collingwood; for here is where the doctrine of the *overlap of classes* is introduced [14, p. 35]:

> Thus art, for the critic, is a highly specialized thing, limited to a small and select body of works outside which lie all the pot-boilers and failures of artists, and the inartistic expressions of everyday life; for the aesthetic philosopher, these too are art, which becomes a thread running all through the fabric of the mind's activity . . . when a concept has a

> dual significance, philosophical and non-philosophical, in its non-philosophical phase it qualifies a limited part of reality, whereas in its philosophical it leaks or escapes out of these limits and invades the neighbouring regions, tending at last to colour our thought of reality as a whole.

1.7 Practice

The leakage of concepts is not very satisfactory for one who likes things tidy. Nonetheless, it happens. In particular, the "inartistic expressions of everyday life" have come to be considered as art by practicing artists.

Danto already knew that art could be considered as immaterial. At least he was aware of the idea, attributed to Harold Rosenberg, "that what abstract painters did was perform an action on a canvas, the way a bullfighter performs an action in the ring" [15, p. 11]. One could let this idea leak out, so that all art would become an act of expression, as it is for Collingwood; but Danto does not seem to have been quite ready for this.

Collingwood spends half of *The Principles of Art* in formulating a sort of definition of art, because the concept needs to be distinguished from overlapping concepts such as craft, amusement, and magic. Craft is doing things with a technique, for a purpose. Craft may *arouse* emotion, either for its own sake, as in amusement, or else, as in *magic,* for something useful beyond itself, such as social control.

Danto mentions some forgeries of Warhol Brillo boxes. Apparently they were intended to deceive, for pecuniary gain, since bidding on authentic Warhol boxes at auction, when possible at all, started at two million dollars [15, p. 50]. Here we are in the realm of magic, where an industry has been created to manipulate feelings about art, and people care about the *provenance* of a box, regardless of whether the box itself helps them to express some artistic feeling.

As I suggested at the beginning, Collingwood did not live to see the term *art* broadened to cover examples like *Brillo Box* that Danto considers. Walking into a building of the University of California at Berkeley, in order hold an informal seminar [15, p. 19],

> I walked past a large classroom which was being painted. The room contained ladders, drop clothes, cans of wall paint and turpentine, and brushes and rollers. I suddenly thought: what if this is an installation titled *Paint Job*?

Danto mentions just such an installation by "the Swiss artistic duo Fischli and Weiss." It seems to me that Danto has the right spirit here. Such installations should be seen as a way to find art in our own ordinary lives.

When I was a sophomore in Santa Fe in 1984–5, at the college called St John's that I have described elsewhere [52], a guest lecturer mentioned an artist who had asked maintenance workers to consider one hour of their daily work as art. Their work could thus have been the kind of thing that Danto imagined in Berkeley as *Paint Job.*

I did not remember the name of the artist, but rediscovered her work in 2013, in the 13th Istanbul Biennial [2, pp. 184–7]. After the labor of giving birth, Mierle Laderman Ukeles came to think of maintenance work as art. She issued *Manifesto for Maintenance Art 1969!* Her work called *I Make Maintenance Art One Hour Every Day* was carried out over seven weeks in 1976 with "300 sky-rise service personnel."

I do not know what those service personnel made of their service as artists. Possibly they acted as if serving a deity, as enjoined by Jesus of Nazareth when describing Judgment Day in Matthew 25:

> 40 And the King shall answer and say unto them, Verily I say unto you, Inasmuch as he have done *it* unto one of the least of my brethren, ye have done *it* unto me.

This is why, as Zooey recalls to Franny, Seymour told him to shine his shoes, even when appearing on a *radio* program, in the story of J. D. Salinger. Zooey should shine his shoes for the Fat Lady [61, pp. 198–200].

> But I'll tell you a terrible secret—*There isn't anyone out there who isn't Seymour's Fat Lady* [. . .] And don't you know—*listen* to me, now—*don't you know who that Fat Lady really is?* . . . Ah, buddy. Ah buddy. It's Christ Himself. Christ Himself, buddy.

Service to a deity is presumably why, by the account of the artist David Macauley that I have remembered from childhood [43, p. 63], in the construction of the cathedral of the make-believe or imaginary town of Chutreaux,

> While the windows were being installed, plasterers covered the underside of the vault and painted red lines on it to give the impression that all the stones of the web were exactly the same size. They were eager for the web to appear perfect even if no one could see the lines from the ground.

God would see the lines.

Workers as artists could add decorative flourishes, as in latte art, or the shamrock in a head of Guinness stout, or a towel rolled into a swan on a hotel bed. Workers might only scrub the floors extra hard, if that is their job. Is this what Mierle Laderman Ukeles had in mind?

At the 1985 show at the Hirshhorn Museum called *Representation Abroad* [62], I was inspired by the Spanish realists Antonio López-Garcia and Isabel Quintanilla to find artistic visions in everyday life, even in a bathroom sink or the corner of a basement. However, Ukeles enjoined maintenance workers not to *see* art, but to *be* artists.

Perhaps one cannot just decide to be an artist. In introducing *Selected Poems of Robert Frost,* Robert Graves writes [30, p. x],

> I agree with Frost that a poem planned beforehand never comes off. Real ones appear unexpectedly, and always at a time when the poet is in a so-called state of grace: which means a clear mind, tense heart, and no worries about fame, money, or other people, but only the excitement of a unique revelation about to be given.

Can one watch for that state of grace, to be ready for it, if it should come?

As he describes in *Surely You're Joking* [26, p. 166], Richard Feynman would seem to have approached the job of teaching as a chance to receive a state of grace.

> If you're teaching a class, you can think about the elementary things that you know very well. These things are kind of fun and delightful. It doesn't do any harm to think them over again. Is there a better way to present them? Are there any new problems associated with them? Are there any new thoughts you can make about them? The elementary things are *easy* to think about; if you can't think of a new thought, no harm done; what you thought about it before is good enough for the class. If you *do* think of something new, you're rather pleased that you have a new way of looking at it.

The present work itself comes out of teaching.

1.8 Numbers

I have taught number theory a few times as an upper-level undergraduate elective, covering arithmetical functions and their convolution, primitive roots of all numbers that have them, and quadratic reciprocity. In the first-year course that I recently taught, I could not go so far. The main aim was for the students to learn about proofs, perhaps for the first time, in the context of real mathematics. The students were doing the same thing concurrently in another course, by reading and presenting to one another the proofs in Book I of Euclid's *Elements,* in the manner of my own aforementioned *alma mater,* St John's College.

In the number-theory course, induction yields the basic form of what we call Fermat's Theorem: for every prime number p, for every number a that it is not itself a multiple of p, the product of $p-1$ instances of a, namely the power a^{p-1}, exceeds by 1 a multiple of p. Playing around with special cases suggests more: that for each prime p, for each of some numbers a called *primitive roots* of p, the power a^{p-1} is the *least* of the powers of a with the indicated property. One can prove this with the help of Euler's φ-function, which counts the numbers less than its argument that are prime to that argument.

I am old enough that pocket calculators started coming out only after I was in school. We still had to learn to use the trig and log tables at the end of our algebra and geometry books [68, 67]. To satisfy my own curiosity, I asked for, and received as a gift, a slide rule from a relative in engineering. To me it is a source of fascination and delight that, using primitive roots, one can compose log tables for *exact* computations.

One can also construct "discrete" slide-rules, corresponding to those tables. I did this for my class, crudely, with the stiff

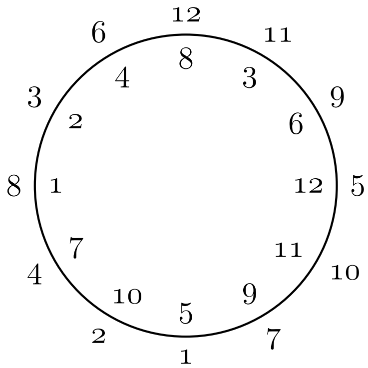


Figure 1.1: Powers of 2 *modulo* 13

cardboard of an old notebook cover, for the small primes 7 and 11; for 13, I cut a circle out of the side of a cardboard box and arranged the numbers like hours on a clockface, as in Figure 1.1, where the dial is set to show multiplication by 5, *modulo* 13. Since 5 and 3 on the inner circle line up with 1 and 11 on the outer circle, 5 times 11 should exceed by 3 a multiple of 13; and this is true, since

$$5 \times 11 = 55 = 4 \times 13 + 3.$$

One could construct similarly a finely machined rotating device, perhaps based on the prime 181, so that the 180 non-congruent non-multiples of this number would be positioned every two degrees.

Such a construction would partake of some of the spirit of Duchamp's *3 Stoppages Etalon (3 Standard Stoppages)* of 1913 [1, pp. 78 f.]:

> Duchamp took three one-metre lengths of string and dropped them from a height of one metre onto a canvas. He then stuck

> the threads down and thereby fixed the new lengths that chance, gravity and the 'whims' of the threads had created . . . Duchamp then proceeded to make three 'rulers' that followed the exact contours of the threads and went on to box them like technical instruments (but in a wooden box resembling a case for croquet sets).

Duchamp's practice may recall what Julian Jaynes describes as "sortilege or the casting of lots . . . designed to provoke the gods' answers to specific questions in novel situations" [36, p. 239]. According to Jaynes's proposal, this is what we did when we could no longer directly hear the voices of the gods [36, p. 236]:

> Subjective consciousness, that is, the development on the basis of linguistic metaphors of an operation space in which an 'I' could narratize out alternative actions to their consequences, was of course the great world result of this dilemma. But a more primitive solution, and one that antedates consciousness as well as paralleling it throughout history, is that complex of behaviors known as divination.

To multiply numbers by means of their discrete logarithms might seem as mysterious as divination.

I may myself be suggesting things that are beyond my comprehension, as artist Bob Deweese thought Robert Pirsig's *alter ego* Phaedrus was doing, in Pirsig's fictionalized recollections in *Zen and the Art of Motorcycle Maintenance* [57, ch. 12, p. 140].

> Phaedrus would say something he thought was pretty funny and DeWeese would look at him in a puzzled way or else take him seriously . . .
>
> For example, there is the fragment of memory about a dining-room table whose edge veneer had come loose and

> which Phaedrus had reglued. He held the veneer in place while the glue set by wrapping a whole ball of string around the table, round and round and round.
>
> DeWeese saw the string and wondered what that was all about.
>
> "That's my latest sculpture," Phaedrus had said. "Don't you think it kind of builds?"
>
> Instead of laughing, DeWeese looked at him with amazement, studied it for a long time and finally said, "Where did you learn all this?" For a second Phaedrus thought he was continuing the joke, but he was serious.

Phaedrus treated modern art flippantly, but practitioners like DeWeese would not do so.

Or perhaps they might. The descriptively titled work called "The first thousand numbers classified in alphabetical order," dated 1989, by Claude Closky [8]—is it a prose poem, or just a joke? One can reconstruct for oneself as much of the work as desired:

> Eight, eight hundred and eight, eight hundred and eighteen, eight hundred and eighty, eight hundred and eighty-eight, eight hundred and eighty-five, eight hundred and eighty-four, eight hundred and eighty-nine, eight hundred and eighty-one, eight hundred and eighty-seven, eight hundred and eighty-six, eight hundred and eighty-three, eight hundred and eighty-two, eight hundred and eleven, . . . two hundred and twelve, two hundred and twenty, two hundred and twenty-eight, two hundred and twenty-five, two hundred and twenty-four, two hundred and twenty-nine, two hundred and twenty-one, two hundred and twenty-seven, two hundred and twenty-six, two hundred and twenty-three, two hundred and twenty-two, two hundred and two.

I seem to recall being taught in the third grade that there was no need to say “and” after the number of hundreds. Thus the 891 instances of this word might be removed from Closky’s work, in an act of what might be called cleaning. Arthur Danto reports that the cleaning of the Sistine Ceiling in the 1990s was thought by some to remove a dimness that had been intended by Michelangelo to suggest the Allegory of the Cave in the *Republic* [15, pp. 55 f.]. Danto himself concludes not.

Meanwhile, back when New Math was the prevalent educational philosophy in the United States, my third-grade classmates and I were also taught to distinguish a *number* from the *numeral* whereby it was expressed. “The first thousand numbers classified in alphabetical order” might be understood to teach the lesson that there *is* a distinction. The lesson would be more explicit if each number, as written out, were followed by its expression in Arabic numerals. This would make Closky’s work notionally useful, like a dictionary.

In 2013, I translated this work, or the *concept* of the work, into Turkish:

> Altı, altı yüz, altı yüz altı, altı yüz altmış, altı yüz altmış altı, altı yüz altmış beş, altı yüz altmış bir, altı yüz altmış dokuz, altı yüz altmış dört, altı yüz altmış iki, altı yüz altmış sekiz, altı yüz altmış üç, altı yüz altmış yedi, altı yüz beş, altı yüz bir, altı yüz doksan, altı yüz doksan altı, . . . yüz yetmiş yedi, yüz yirmi, yüz yirmi altı, yüz yirmi beş, yüz yirmi bir, yüz yirmi dokuz, yüz yirmi dört, yüz yirmi iki, yüz yirmi sekiz, yüz yirmi üç, yüz yirmi yedi.

Then I created a dictionary of Roman numerals, summarized in Table 1.2. One who knows Roman numerals may recognize that the greatest Roman numeral in the dictionary is MMMCMXCIX; but this is entry number 3241. One who never got the hang of Roman numerals might conceivably find the dictionary useful. I even allowed the MakeIndex program that

1.	C	100
2.	CC	200
3.	CCC	300
4.	CCCI	301
5.	CCCII	302
6.	CCCIII	303
7.	CCCIV	304
8.	CCCIX	309
9.	CCCL	350
10.	CCCLI	351
11.	CCCLII	352
12.	CCCLIII	353
13.	CCCLIV	354
14.	CCCLIX	359
...	...	...
3986.	XXV	25
3987.	XXVI	26
3988.	XXVII	27
3989.	XXVIII	28
3990.	XXX	30
3991.	XXXI	31
3992.	XXXII	32
3993.	XXXIII	33
3994.	XXXIV	34
3995.	XXXIX	39
3996.	XXXV	35
3997.	XXXVI	36
3998.	XXXVII	37
3999.	XXXVIII	38

Table 1.2: Roman numerals in alphabetical order

accompanies LaTeX to produce an index of the page number where each Arabic numeral appeared.

There was a dictionary in the 12th Istanbul Biennial, in 2011. Born in Istanbul, living in Stockholm, Meriç Algün Ringborg created *Ö (The Mutual Letter),* a Swedish-Turkish dictionary, consisting only of the 1270 words that are spelled the same in Turkish as in Swedish [35, p. 252]. Some of the words feature the letter Ö, which is common to the two languages, though it has different places in the alphabetical order; in Turkish it lies between O and P. Distributed as a saddle-bound booklet of 40 blue pages of size A6, the dictionary is summarized in Table 1.3. The artist stresses that, despite appearances, the paired words belong to different languages and are pronounced accordingly; she suggests that this could be heard in the aural component of the display in the Biennial, though I do not personally remember it.

Before passing to the logarithm "dictionaries" or tables of Chapter 2, let me quote them too elliptically, as in Table 1.4. The need for a distinct table of antilogarithms (at least if practical use is contemplated) should be contrasted with the case of common logarithms, which proceed in order as in Table 1.5 [68, pp. 606 f.]. Gaps can be filled in as finely as wished, as for example in Table 1.6. But the number of discrete logarithms is fixed by the modulus that they are based on—997, in the next chapter.

abdomen abdomen
abdominal abdominal
abort abort
abrakadabra abrakadabra
absorbent absorbent
adenin adenin
adenit adenit
adenoid adenoid
adenom adenom
adrenalin adrenalin
aerosol aerosol
agoni agoni
agorafobi agorafobi
agronomi agronomi
. . . .
vokalist vokalist
volt volt
volta volta
yen yen
yoga yoga
zebra zebra
zenit zenit
zeolit zeolit
zirkon zirkon
zon zon
zoolog zoolog
zootomi zootomi
ödem ödem
östron östron

Table 1.3: Algün Ringborg, *Ö (The Mutual Letter)*

logarithms		antilogs	
2.	201	1.	7
3.	6	2.	49
4.	402	3.	343
5.	465	4.	407
6.	207	5.	855
7.	1	6.	3
8.	603	7.	21
9.	12	8.	147
10.	666	9.	32
11.	817	10.	224
12.	408	11.	571
13.	580	12.	9
14.	202	13.	63
15.	471	14.	441
....		....	
983.	700	982.	52
984.	82	983.	364
985.	906	984.	554
986.	319	985.	887
987.	168	986.	227
988.	510	987.	592
989.	105	988.	156
990.	499	989.	95
991.	705	990.	665
992.	963	991.	667
993.	900	992.	681
994.	504	993.	779
995.	699	994.	468
996.	498	995.	285

Table 1.4: Discrete logarithms

N	$\log N$
1	0.0000
2	0.3010
3	0.4771
4	0.6021
5	0.6990
6	0.7782
7	0.8451
8	0.9031
9	0.9542
10	1.0000

Table 1.5: Common logarithms, coarsely

N	$\log N$	N	$\log N$	N	$\log N$	N	$\log N$
1.00	0.0000	1.10	0.0414	1.20	0.0792	9.90	0.9956
1.01	0.0043	1.11	0.0453	1.21	0.0828	9.91	0.9961
1.02	0.0086	1.12	0.0492	1.22	0.0864	9.92	0.9965
1.03	0.0128	1.13	0.0531	1.23	0.0899	9.93	0.9969
1.04	0.0170	1.14	0.0569	1.24	0.0934	9.94	0.9974
1.05	0.0212	1.15	0.0607	. . . . . .	. . . . . .	9.95	0.9978
1.06	0.0253	1.16	0.0645	9.86	0.9939	9.96	0.9983
1.07	0.0294	1.17	0.0682	9.87	0.9943	9.97	0.9987
1.08	0.0334	1.18	0.0719	9.88	0.9948	9.98	0.9991
1.09	0.0374	1.19	0.0755	9.89	0.9952	9.99	0.9996

Table 1.6: Common logarithms, finely

2 Tables

2.1 Logarithms

2.	201	23.	248	44.	223	65.	49	86.	58
3.	6	24.	609	45.	477	66.	28	87.	749
4.	402	25.	930	46.	449	67.	132	88.	424
5.	465	26.	781	47.	161	68.	773	89.	890
6.	207	27.	18	48.	810	69.	254	90.	678
7.	1	28.	403	49.	2	70.	667	91.	581
8.	603	29.	743	50.	135	71.	302	92.	650
9.	12	30.	672	51.	377	72.	615	93.	960
10.	666	31.	954	52.	982	73.	728	94.	362
11.	817	32.	9	53.	142	74.	384	95.	989
12.	408	33.	823	54.	219	75.	936	96.	15
13.	580	34.	572	55.	286	76.	926	97.	846
14.	202	35.	466	56.	604	77.	818	98.	203
15.	471	36.	414	57.	530	78.	787	99.	829
16.	804	37.	183	58.	944	79.	92	100.	336
17.	371	38.	725	59.	832	80.	273	101.	910
18.	213	39.	586	60.	873	81.	24	102.	578
19.	524	40.	72	61.	697	82.	670	103.	157
20.	867	41.	469	62.	159	83.	90	104.	187
21.	7	42.	208	63.	13	84.	409	105.	472
22.	22	43.	853	64.	210	85.	836	106.	343

107.	62	139.	110	171.	536	203.	744	235.	626
108.	420	140.	868	172.	259	204.	779	236.	238
109.	294	141.	167	173.	262	205.	934	237.	98
110.	487	142.	503	174.	950	206.	358	238.	573
111.	189	143.	401	175.	931	207.	260	239.	565
112.	805	144.	816	176.	625	208.	388	240.	279
113.	855	145.	212	177.	838	209.	345	241.	919
114.	731	146.	929	178.	95	210.	673	242.	839
115.	713	147.	8	179.	611	211.	479	243.	30
116.	149	148.	585	180.	879	212.	544	244.	103
117.	592	149.	448	181.	683	213.	308	245.	467
118.	37	150.	141	182.	782	214.	263	246.	676
119.	372	151.	872	183.	703	215.	322	247.	108
120.	78	152.	131	184.	851	216.	621	248.	561
121.	638	153.	383	185.	648	217.	955	249.	96
122.	898	154.	23	186.	165	218.	495	250.	600
123.	475	155.	423	187.	192	219.	734	251.	595
124.	360	156.	988	188.	563	220.	688	252.	415
125.	399	157.	577	189.	19	221.	951	253.	69
126.	214	158.	293	190.	194	222.	390	254.	122
127.	917	159.	148	191.	241	223.	568	255.	842
128.	411	160.	474	192.	216	224.	10	256.	612
129.	859	161.	249	193.	42	225.	942	257.	552
130.	250	162.	225	194.	51	226.	60	258.	64
131.	770	163.	815	195.	55	227.	986	259.	184
132.	229	164.	871	196.	404	228.	932	260.	451
133.	525	165.	292	197.	441	229.	120	261.	755
134.	333	166.	291	198.	34	230.	914	262.	971
135.	483	167.	258	199.	234	231.	824	263.	880
136.	974	168.	610	200.	537	232.	350	264.	430
137.	226	169.	164	201.	138	233.	145	265.	607
138.	455	170.	41	202.	115	234.	793	266.	726

267.	896	299.	828	331.	894	363.	644	395.	557
268.	534	300.	342	332.	492	364.	983	396.	235
269.	686	301.	854	333.	195	365.	197	397.	45
270.	684	302.	77	334.	459	366.	904	398.	435
271.	347	303.	916	335.	597	367.	181	399.	531
272.	179	304.	332	336.	811	368.	56	400.	738
273.	587	305.	166	337.	196	369.	481	401.	352
274.	427	306.	584	338.	365	370.	849	402.	339
275.	751	307.	422	339.	861	371.	143	403.	538
276.	656	308.	224	340.	242	372.	366	404.	316
277.	783	309.	163	341.	775	373.	892	405.	489
278.	311	310.	624	342.	737	374.	393	406.	945
279.	966	311.	702	343.	3	375.	405	407.	4
280.	73	312.	193	344.	460	376.	764	408.	980
281.	515	313.	440	345.	719	377.	327	409.	908
282.	368	314.	778	346.	463	378.	220	410.	139
283.	81	315.	478	347.	217	379.	862	411.	232
284.	704	316.	494	348.	155	380.	395	412.	559
285.	995	317.	941	349.	129	381.	923	413.	833
286.	602	318.	349	350.	136	382.	442	414.	461
287.	470	319.	564	351.	598	383.	125	415.	555
288.	21	320.	675	352.	826	384.	417	416.	589
289.	742	321.	68	353.	153	385.	287	417.	116
290.	413	322.	450	354.	43	386.	243	418.	546
291.	852	323.	895	355.	767	387.	865	419.	445
292.	134	324.	426	356.	296	388.	252	420.	874
293.	529	325.	514	357.	378	389.	35	421.	720
294.	209	326.	20	358.	812	390.	256	422.	680
295.	301	327.	300	359.	267	391.	619	423.	173
296.	786	328.	76	360.	84	392.	605	424.	745
297.	835	329.	162	361.	52	393.	776	425.	305
298.	649	330.	493	362.	884	394.	642	426.	509

427.	698	459.	389	491.	768	523.	797	555.	654
428.	464	460.	119	492.	877	524.	176	556.	512
429.	407	461.	237	493.	118	525.	937	557.	391
430.	523	462.	29	494.	309	526.	85	558.	171
431.	780	463.	599	495.	298	527.	329	559.	437
432.	822	464.	551	496.	762	528.	631	560.	274
433.	71	465.	429	497.	303	529.	496	561.	198
434.	160	466.	346	498.	297	530.	808	562.	716
435.	218	467.	310	499.	795	531.	844	563.	658
436.	696	468.	994	500.	801	532.	927	564.	569
437.	772	469.	133	501.	264	533.	53	565.	324
438.	935	470.	827	502.	796	534.	101	566.	282
439.	669	471.	583	503.	807	535.	527	567.	25
440.	889	472.	439	504.	616	536.	735	568.	905
441.	14	473.	674	505.	379	537.	617	569.	962
442.	156	474.	299	506.	270	538.	887	570.	200
443.	486	475.	458	507.	170	539.	819	571.	11
444.	591	476.	774	508.	323	540.	885	572.	803
445.	359	477.	154	509.	802	541.	635	573.	247
446.	769	478.	766	510.	47	542.	548	574.	671
447.	454	479.	883	511.	729	543.	689	575.	182
448.	211	480.	480	512.	813	544.	380	576.	222
449.	130	481.	763	513.	542	545.	759	577.	376
450.	147	482.	124	514.	753	546.	788	578.	943
451.	290	483.	255	515.	622	547.	645	579.	48
452.	261	484.	44	516.	265	548.	628	580.	614
453.	878	485.	315	517.	978	549.	709	581.	91
454.	191	486.	231	518.	385	550.	952	582.	57
455.	50	487.	545	519.	268	551.	271	583.	959
456.	137	488.	304	520.	652	552.	857	584.	335
457.	387	489.	821	521.	276	553.	93	585.	61
458.	321	490.	668	522.	956	554.	984	586.	730

587.	637	619.	718	651.	961	683.	280	715.	866
588.	410	620.	825	652.	221	684.	938	716.	17
589.	482	621.	266	653.	958	685.	691	717.	571
590.	502	622.	903	654.	501	686.	204	718.	468
591.	447	623.	891	655.	239	687.	126	719.	809
592.	987	624.	394	656.	277	688.	661	720.	285
593.	814	625.	864	657.	740	689.	722	721.	158
594.	40	626.	641	658.	363	690.	920	722.	253
595.	837	627.	351	659.	863	691.	86	723.	925
596.	850	628.	979	660.	694	692.	664	724.	89
597.	240	629.	554	661.	313	693.	830	725.	677
598.	33	630.	679	662.	99	694.	418	726.	845
599.	933	631.	406	663.	957	695.	575	727.	186
600.	543	632.	695	664.	693	696.	356	728.	188
601.	733	633.	485	665.	990	697.	840	729.	36
602.	59	634.	146	666.	396	698.	330	730.	398
603.	144	635.	386	667.	991	699.	151	731.	228
604.	278	636.	550	668.	660	700.	337	732.	109
605.	107	637.	582	669.	574	701.	288	733.	928
606.	121	638.	765	670.	798	702.	799	734.	382
607.	754	639.	314	671.	518	703.	707	735.	473
608.	533	640.	876	672.	16	704.	31	736.	257
609.	750	641.	794	673.	924	705.	632	737.	949
610.	367	642.	269	674.	397	706.	354	738.	682
611.	741	643.	541	675.	948	707.	911	739.	562
612.	785	644.	651	676.	566	708.	244	740.	54
613.	915	645.	328	677.	177	709.	519	741.	114
614.	623	646.	100	678.	66	710.	968	742.	344
615.	940	647.	634	679.	847	711.	104	743.	620
616.	425	648.	627	680.	443	712.	497	744.	567
617.	893	649.	653	681.	992	713.	206	745.	913
618.	364	650.	715	682.	976	714.	579	746.	97

747.	102	779.	993	811.	663	843.	521	875.	400
748.	594	780.	457	812.	150	844.	881	876.	140
749.	63	781.	123	813.	353	845.	629	877.	576
750.	606	782.	820	814.	205	846.	374	878.	870
751.	178	783.	761	815.	284	847.	639	879.	535
752.	965	784.	806	816.	185	848.	946	880.	94
753.	601	785.	46	817.	381	849.	87	881.	647
754.	528	786.	977	818.	113	850.	506	882.	215
755.	341	787.	175	819.	593	851.	431	883.	233
756.	421	788.	843	820.	340	852.	710	884.	357
757.	777	789.	886	821.	127	853.	318	885.	307
758.	67	790.	758	822.	433	854.	899	886.	687
759.	75	791.	856	823.	452	855.	5	887.	985
760.	596	792.	436	824.	760	856.	665	888.	792
761.	736	793.	281	825.	757	857.	370	889.	918
762.	128	794.	246	826.	38	858.	608	890.	560
763.	295	795.	613	827.	539	859.	953	891.	841
764.	643	796.	636	828.	662	860.	724	892.	970
765.	848	797.	39	829.	112	861.	476	893.	685
766.	326	798.	732	830.	756	862.	981	894.	655
767.	416	799.	532	831.	789	863.	831	895.	80
768.	618	800.	939	832.	790	864.	27	896.	412
769.	434	801.	902	833.	373	865.	727	897.	834
770.	488	802.	553	834.	317	866.	272	898.	331
771.	558	803.	549	835.	723	867.	748	899.	701
772.	444	804.	540	836.	747	868.	361	900.	348
773.	508	805.	714	837.	972	869.	909	901.	513
774.	70	806.	739	838.	646	870.	419	902.	491
775.	888	807.	692	839.	791	871.	712	903.	860
776.	453	808.	517	840.	79	872.	897	904.	462
777.	190	809.	65	841.	490	873.	858	905.	152
778.	236	810.	690	842.	921	874.	973	906.	83

907.	180	925.	117	943.	717	961.	912	979.	711
908.	392	926.	800	944.	640	962.	964	980.	869
909.	922	927.	169	945.	484	963.	74	981.	306
910.	251	928.	752	946.	875	964.	325	982.	969
911.	556	929.	275	947.	633	965.	507	983.	700
912.	338	930.	630	948.	500	966.	456	984.	82
913.	907	931.	526	949.	312	967.	174	985.	906
914.	588	932.	547	950.	659	968.	245	986.	319
915.	172	933.	708	951.	947	969.	901	987.	168
916.	522	934.	511	952.	975	970.	516	988.	510
917.	771	935.	657	953.	721	971.	283	989.	105
918.	590	936.	199	954.	355	972.	432	990.	499
919.	289	937.	375	955.	706	973.	111	991.	705
920.	320	938.	334	956.	967	974.	746	992.	963
921.	428	939.	446	957.	570	975.	520	993.	900
922.	438	940.	32	958.	88	976.	505	994.	504
923.	882	941.	106	959.	227	977.	369	995.	699
924.	230	942.	784	960.	681	978.	26	996.	498

2.2 Antilogarithms

1.	7	10.	224	19.	189	28.	66	37.	118
2.	49	11.	571	20.	326	29.	462	38.	826
3.	343	12.	9	21.	288	30.	243	39.	797
4.	407	13.	63	22.	22	31.	704	40.	594
5.	855	14.	441	23.	154	32.	940	41.	170
6.	3	15.	96	24.	81	33.	598	42.	193
7.	21	16.	672	25.	567	34.	198	43.	354
8.	147	17.	716	26.	978	35.	389	44.	484
9.	32	18.	27	27.	864	36.	729	45.	397

46.	785	78.	120	110.	139	142.	53	174.	967
47.	510	79.	840	111.	973	143.	371	175.	787
48.	579	80.	895	112.	829	144.	603	176.	524
49.	65	81.	283	113.	818	145.	233	177.	677
50.	455	82.	984	114.	741	146.	634	178.	751
51.	194	83.	906	115.	202	147.	450	179.	272
52.	361	84.	360	116.	417	148.	159	180.	907
53.	533	85.	526	117.	925	149.	116	181.	367
54.	740	86.	691	118.	493	150.	812	182.	575
55.	195	87.	849	119.	460	151.	699	183.	37
56.	368	88.	958	120.	229	152.	905	184.	259
57.	582	89.	724	121.	606	153.	353	185.	816
58.	86	90.	83	122.	254	154.	477	186.	727
59.	602	91.	581	123.	781	155.	348	187.	104
60.	226	92.	79	124.	482	156.	442	188.	728
61.	585	93.	553	125.	383	157.	103	189.	111
62.	107	94.	880	126.	687	158.	721	190.	777
63.	749	95.	178	127.	821	159.	62	191.	454
64.	258	96.	249	128.	762	160.	434	192.	187
65.	809	97.	746	129.	349	161.	47	193.	312
66.	678	98.	237	130.	449	162.	329	194.	190
67.	758	99.	662	131.	152	163.	309	195.	333
68.	321	100.	646	132.	67	164.	169	196.	337
69.	253	101.	534	133.	469	165.	186	197.	365
70.	774	102.	747	134.	292	166.	305	198.	561
71.	433	103.	244	135.	50	167.	141	199.	936
72.	40	104.	711	136.	350	168.	987	200.	570
73.	280	105.	989	137.	456	169.	927	201.	2
74.	963	106.	941	138.	201	170.	507	202.	14
75.	759	107.	605	139.	410	171.	558	203.	98
76.	328	108.	247	140.	876	172.	915	204.	686
77.	302	109.	732	141.	150	173.	423	205.	814

206.	713	238.	236	270.	506	302.	71	334.	938
207.	6	239.	655	271.	551	303.	497	335.	584
208.	42	240.	597	272.	866	304.	488	336.	100
209.	294	241.	191	273.	80	305.	425	337.	700
210.	64	242.	340	274.	560	306.	981	338.	912
211.	448	243.	386	275.	929	307.	885	339.	402
212.	145	244.	708	276.	521	308.	213	340.	820
213.	18	245.	968	277.	656	309.	494	341.	755
214.	126	246.	794	278.	604	310.	467	342.	300
215.	882	247.	573	279.	240	311.	278	343.	106
216.	192	248.	23	280.	683	312.	949	344.	742
217.	347	249.	161	281.	793	313.	661	345.	209
218.	435	250.	130	282.	566	314.	639	346.	466
219.	54	251.	910	283.	971	315.	485	347.	271
220.	378	252.	388	284.	815	316.	404	348.	900
221.	652	253.	722	285.	720	317.	834	349.	318
222.	576	254.	69	286.	55	318.	853	350.	232
223.	44	255.	483	287.	385	319.	986	351.	627
224.	308	256.	390	288.	701	320.	920	352.	401
225.	162	257.	736	289.	919	321.	458	353.	813
226.	137	258.	167	290.	451	322.	215	354.	706
227.	959	259.	172	291.	166	323.	508	355.	954
228.	731	260.	207	292.	165	324.	565	356.	696
229.	132	261.	452	293.	158	325.	964	357.	884
230.	924	262.	173	294.	109	326.	766	358.	206
231.	486	263.	214	295.	763	327.	377	359.	445
232.	411	264.	501	296.	356	328.	645	360.	124
233.	883	265.	516	297.	498	329.	527	361.	868
234.	199	266.	621	298.	495	330.	698	362.	94
235.	396	267.	359	299.	474	331.	898	363.	658
236.	778	268.	519	300.	327	332.	304	364.	618
237.	461	269.	642	301.	295	333.	134	365.	338

366.	372	398.	730	430.	264	462.	904	494.	316
367.	610	399.	125	431.	851	463.	346	495.	218
368.	282	400.	875	432.	972	464.	428	496.	529
369.	977	401.	143	433.	822	465.	5	497.	712
370.	857	402.	4	434.	769	466.	35	498.	996
371.	17	403.	28	435.	398	467.	245	499.	990
372.	119	404.	196	436.	792	468.	718	500.	948
373.	833	405.	375	437.	559	469.	41	501.	654
374.	846	406.	631	438.	922	470.	287	502.	590
375.	937	407.	429	439.	472	471.	15	503.	142
376.	577	408.	12	440.	313	472.	105	504.	994
377.	51	409.	84	441.	197	473.	735	505.	976
378.	357	410.	588	442.	382	474.	160	506.	850
379.	505	411.	128	443.	680	475.	123	507.	965
380.	544	412.	896	444.	772	476.	861	508.	773
381.	817	413.	290	445.	419	477.	45	509.	426
382.	734	414.	36	446.	939	478.	315	510.	988
383.	153	415.	252	447.	591	479.	211	511.	934
384.	74	416.	767	448.	149	480.	480	512.	556
385.	518	417.	384	449.	46	481.	369	513.	901
386.	635	418.	694	450.	322	482.	589	514.	325
387.	457	419.	870	451.	260	483.	135	515.	281
388.	208	420.	108	452.	823	484.	945	516.	970
389.	459	421.	756	453.	776	485.	633	517.	808
390.	222	422.	307	454.	447	486.	443	518.	671
391.	557	423.	155	455.	138	487.	110	519.	709
392.	908	424.	88	456.	966	488.	770	520.	975
393.	374	425.	616	457.	780	489.	405	521.	843
394.	624	426.	324	458.	475	490.	841	522.	916
395.	380	427.	274	459.	334	491.	902	523.	430
396.	666	428.	921	460.	344	492.	332	524.	19
397.	674	429.	465	461.	414	493.	330	525.	133

526.	931	558.	771	590.	918	622.	515	654.	555
527.	535	559.	412	591.	444	623.	614	655.	894
528.	754	560.	890	592.	117	624.	310	656.	276
529.	293	561.	248	593.	819	625.	176	657.	935
530.	57	562.	739	594.	748	626.	235	658.	563
531.	399	563.	188	595.	251	627.	648	659.	950
532.	799	564.	319	596.	760	628.	548	660.	668
533.	608	565.	239	597.	335	629.	845	661.	688
534.	268	566.	676	598.	351	630.	930	662.	828
535.	879	567.	744	599.	463	631.	528	663.	811
536.	171	568.	223	600.	250	632.	705	664.	692
537.	200	569.	564	601.	753	633.	947	665.	856
538.	403	570.	957	602.	286	634.	647	666.	10
539.	827	571.	717	603.	8	635.	541	667.	70
540.	804	572.	34	604.	56	636.	796	668.	490
541.	643	573.	238	605.	392	637.	587	669.	439
542.	513	574.	669	606.	750	638.	121	670.	82
543.	600	575.	695	607.	265	639.	847	671.	574
544.	212	576.	877	608.	858	640.	944	672.	30
545.	487	577.	157	609.	24	641.	626	673.	210
546.	418	578.	102	610.	168	642.	394	674.	473
547.	932	579.	714	611.	179	643.	764	675.	320
548.	542	580.	13	612.	256	644.	363	676.	246
549.	803	581.	91	613.	795	645.	547	677.	725
550.	636	582.	637	614.	580	646.	838	678.	90
551.	464	583.	471	615.	72	647.	881	679.	630
552.	257	584.	306	616.	504	648.	185	680.	422
553.	802	585.	148	617.	537	649.	298	681.	960
554.	629	586.	39	618.	768	650.	92	682.	738
555.	415	587.	273	619.	391	651.	644	683.	181
556.	911	588.	914	620.	743	652.	520	684.	270
557.	395	589.	416	621.	216	653.	649	685.	893

686.	269	718.	619	750.	609	782.	182	814.	593
687.	886	719.	345	751.	275	783.	277	815.	163
688.	220	720.	421	752.	928	784.	942	816.	144
689.	543	721.	953	753.	514	785.	612	817.	11
690.	810	722.	689	754.	607	786.	296	818.	77
691.	685	723.	835	755.	261	787.	78	819.	539
692.	807	724.	860	756.	830	788.	546	820.	782
693.	664	725.	38	757.	825	789.	831	821.	489
694.	660	726.	266	758.	790	790.	832	822.	432
695.	632	727.	865	759.	545	791.	839	823.	33
696.	436	728.	73	760.	824	792.	888	824.	231
697.	61	729.	511	761.	783	793.	234	825.	620
698.	427	730.	586	762.	496	794.	641	826.	352
699.	995	731.	114	763.	481	795.	499	827.	470
700.	983	732.	798	764.	376	796.	502	828.	299
701.	899	733.	601	765.	638	797.	523	829.	99
702.	311	734.	219	766.	478	798.	670	830.	693
703.	183	735.	536	767.	355	799.	702	831.	863
704.	284	736.	761	768.	491	800.	926	832.	59
705.	991	737.	342	769.	446	801.	500	833.	413
706.	955	738.	400	770.	131	802.	509	834.	897
707.	703	739.	806	771.	917	803.	572	835.	297
708.	933	740.	657	772.	437	804.	16	836.	85
709.	549	741.	611	773.	68	805.	112	837.	595
710.	852	742.	289	774.	476	806.	784	838.	177
711.	979	743.	29	775.	341	807.	503	839.	242
712.	871	744.	203	776.	393	808.	530	840.	697
713.	115	745.	424	777.	757	809.	719	841.	891
714.	805	746.	974	778.	314	810.	48	842.	255
715.	650	747.	836	779.	204	811.	336	843.	788
716.	562	748.	867	780.	431	812.	358	844.	531
717.	943	749.	87	781.	26	813.	512	845.	726

846.	97	876.	640	906.	985	936.	75	966.	279
847.	679	877.	492	907.	913	937.	525	967.	956
848.	765	878.	453	908.	409	938.	684	968.	710
849.	370	879.	180	909.	869	939.	800	969.	982
850.	596	880.	263	910.	101	940.	615	970.	892
851.	184	881.	844	911.	707	941.	317	971.	262
852.	291	882.	923	912.	961	942.	225	972.	837
853.	43	883.	479	913.	745	943.	578	973.	874
854.	301	884.	362	914.	230	944.	58	974.	136
855.	113	885.	540	915.	613	945.	406	975.	952
856.	791	886.	789	916.	303	946.	848	976.	682
857.	552	887.	538	917.	127	947.	951	977.	786
858.	873	888.	775	918.	889	948.	675	978.	517
859.	129	889.	440	919.	241	949.	737	979.	628
860.	903	890.	89	920.	690	950.	174	980.	408
861.	339	891.	623	921.	842	951.	221	981.	862
862.	379	892.	373	922.	909	952.	550	982.	52
863.	659	893.	617	923.	381	953.	859	983.	364
864.	625	894.	331	924.	673	954.	31	984.	554
865.	387	895.	323	925.	723	955.	217	985.	887
866.	715	896.	267	926.	76	956.	522	986.	227
867.	20	897.	872	927.	532	957.	663	987.	592
868.	140	898.	122	928.	733	958.	653	988.	156
869.	980	899.	854	929.	146	959.	583	989.	95
870.	878	900.	993	930.	25	960.	93	990.	665
871.	164	901.	969	931.	175	961.	651	991.	667
872.	151	902.	801	932.	228	962.	569	992.	681
873.	60	903.	622	933.	599	963.	992	993.	779
874.	420	904.	366	934.	205	964.	962	994.	468
875.	946	905.	568	935.	438	965.	752	995.	285

3 Mathematics

3.1 Practice and Theory

In Chapter 2, if the entry $\boxed{x. \quad y}$ appears in the table of logarithms (§2.1), or $\boxed{y. \quad x}$ in the table of antilogarithms (§2.2), let us write

$$\log x = y.$$

As suggested in the Introduction, this means

$$7^y \equiv x \pmod{997},$$

in Gauss's notation for congruence, defined in this chapter. Suppose in particular that the product of two numbers a and b, each less than 997, is desired. One can find the product as follows.

1. Look up $\log a$ and $\log b$.
2. Compute the sum $\log a + \log b$.
3. If this sum exceeds 996, subtract the latter.
4. Look up the antilogarithm of the result.

The number so obtained is either the product ab of the original numbers or else its remainder after division by 997.

For example:

1. The logarithms of 23 and 31 are 248 and 954.
2. The sum of 248 and 954 is 1202.
3. This, less 996, is 206.

4. The antilogarithm of this is 713, which is 23 times 31.

The rest of this chapter shows why this procedure is possible. In principle, the review should be mostly accessible to the interested layperson. In practice, the material might take several weeks of study. Any reader must tolerate some quotations (accompanied by translations) in Greek, Latin, and French. For the mathematics itself, a contemporary textbook is Burton's *Elementary Number Theory* [6], but everything is found—in Latin, originally—in Gauss's *Disquisitiones Arithmeticae* [32].

The treatment of discrete logarithms given here is terser than the laborious exposition of common logarithms in Isaac Asimov's 1965 *Easy Introduction to the Slide Rule.* On the other hand, Asimov tacitly requires the reader to accept, for example, that the number 10 has a square root [3, p. 49]. This number is *approximated* by 3.162120, and the reader is supposed to be able to verify, by hand, that the square of this number is 9.9990028944. (I have actually done this.)

Agreeing with David Fowler [27], I think Dedekind was right to say in the 1880s [16, pp. 22, 40] that he had been the first to *prove,* as a consequence of the construction of the real numbers, the existence of square roots, along with the rule for their multiplication, whereby, for example,

$$\sqrt{2} \cdot \sqrt{3} = \sqrt{6}.$$

One can give a geometrical argument for this particular equation, as in Figure 3.1, where ABC is an isosceles right triangle, and CD is drawn perpendicular to AC and equal to CB, and $AE = AD$, and the perpendicular to AE at E meets the extension of AC at F. If AB and therefore BC and CD are each counted as a unit, then AC has length $\sqrt{2}$, and so AD has length $\sqrt{3}$. Since again $AE = AD$, and AEF is isosceles, we conclude that AF, as hypoteneuse of AEF, has length

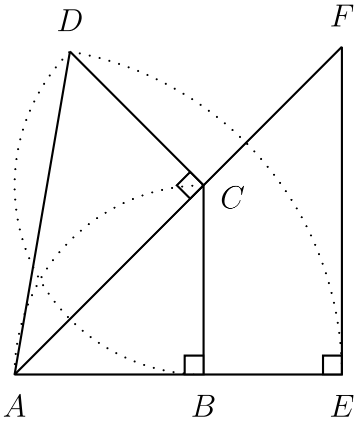


Figure 3.1: $\sqrt{2} \cdot \sqrt{3} = \sqrt{6}$

$\sqrt{6}$. By similar triangles and the result concerning them called Thales's Theorem (mentioned also later, on page 66), AF also has length $\sqrt{2} \cdot \sqrt{3}$. However, this conclusion assumes the geometrical theory of multiplication suggested by Descartes in his *Géometrie* [17], but not rigorously justified, as far as I know, until the 1890s, in Hilbert's *Foundations of Geometry* [34].

Such theoretical matters are beyond Asimov's scope. They would not be beyond my scope, if common logarithms rather than discrete logarithms were my subject. I start with the question of what a number is in the first place.

3.2 Numbers

The second mathematical activity of our lives is to count. The first is to recognize the existence of such individuals or unities as *can* be counted.

Let us understand a **number** as a collection whose members can be counted. This would seem to be the sense of number in Euclid's *Elements* [21], where, at the head of Book VII, a number is said to be a multitude of individuals, or unities, or (transliterating the Greek) monads. John Dee invented the word *unit,* precisely to translate Euclid's *ἡ μονάς -άδος* [55, §2.5].

Euclid's numbers might be understood as being what in modern terms are *finite sets.* When two sets are in one-to-one correspondence, today we may say that they are *equipollent*; for Euclid they are simply **equal** as numbers, just as, by definition, two distinct sides of an isosceles triangle (like AB and BC in Figure 3.1) are equal as bounded straight lines. This is the meaning of the Greek adjective *ἰσοσκελής -ές*, which combines *ἴσος -η -ον* *equal* with *τό σκέλος -ους* *leg.* In Euclid's diagrams, a number is such a bounded straight line as is implicitly divisible into units, all being equal to one another or, in modern terms, having the same length.

3.3 Multiplication

It is possible to **multiply** one number, the **multiplicand,** by another number, the **multiplier.** This means to lay out the multiplicand as many times as there are units in the multiplier, so that a new number is obtained. The new number is the **multiple** of the multiplicand by the multiplier. It is also the **product** of these two numbers, if we know which is which.

To obtain a product, what we lay out is perhaps not strictly the multiplicand itself, but *copies* of it, namely numbers that are equal to it. The distinction is lost in our notation. Five times six would appear to be, literally, six, laid out five times; this gives

$$6+6+6+6+6,$$

the sum we know as 30. I propose to denote the product here as $6 \cdot 5$, to be understood as six, multiplied by five.

The multiplicand **measures** the product and is a **submultiple** of it; the multiplier **divides** the product. We can measure thirty apples by six apples: the result is five piles, each holding six apples. This means we can divide the thirty apples among five children: each child gets six apples. Without using this terminology, Alexandre Borovik discusses the distinction between measuring and dividing apples in *Metamathematics of Elementary Mathematics* [5].

Using the results just discussed, how can we show that the thirty apples can *also* be divided among six children? Why should the sum

$$5 + 5 + 5 + 5 + 5 + 5$$

of six fives be equal to the sum of five sixes as above? Why should the product of two numbers be the same, regardless of which of the two numbers is multiplicand, and which is multiplier? Why should these two numbers be indifferently the **factors** of the product?

We shall review Euclid's general proof of what we call the **commutativity** of multiplication: that property whereby, if the roles of multiplicand and multiplier among two factors are interchanged, the product is unchanged. The proof will involve *ratios* of numbers.

3.4 The Euclidean Algorithm

Given a pair of numbers, we may transform it by subtracting the less from the greater. We can continue until the two numbers become equal. We call this process the **Euclidean Algorithm.** In the first two propositions of Book VII of the

Elements [22], Euclid describes the process with the passive form of the verb *ἀνθυφαιρέω*, *to take away alternately.* It is a deficiency of the big Liddell–Scott–Jones lexicon [42] that Euclid is not cited under this word, from which can be derived the noun *anthyphaeresis* (*ἀνθυφαίρεσις*), meaning *alternate subtraction.*

At the end of the anthyphaeresis, either of the two equal numbers measures all of the numbers that came before, and so it is in particular a **common measure** of the original two numbers. Moreover, every common measure of these numbers measures every number found in the course of the anthyphaeresis; in particular, the common measure measures the last number, which is therefore the **greatest common measure** of the first two numbers. In the case where this greatest common measure is properly speaking not a number but a single unit, the two original numbers must be **prime to one another.**

I once considered teaching number theory on the pattern of Euclid, but then I found his approach too strange for the modern student. I did learn two things: (1) the implicit use of the Euclidean algorithm in the definition of proportion of numbers, and (2) the use of this definition in a rigorous proof of commutativity of multiplication.

Suppose we apply the Euclidean Algorithm to two numbers, lying on the left and right respectively. At each step of the algorithm, we record first whether the left-hand or right-hand number is greater. Thus we may obtain a sequence of letters L and R. If this is the same as the sequence obtained from another pair of numbers, then, by Euclid's definition at the head of Book VII, the four numbers are **in proportion,** and the first two numbers have the **same ratio** as the second two numbers.

Let us pass to modern symbolism in an example. If the first two numbers are 14 and 10, then the steps of the algorithm give us

$$(14, 10), \qquad (4, 10), \qquad (4, 6), \qquad (4, 2), \qquad (2, 2),$$

whence 2 is the greatest common measure of 14 and 10. From 21 and 15 we obtain

$$(21, 15), \qquad (6, 15), \qquad (6, 9), \qquad (6, 3), \qquad (3, 3),$$

so 3 is the greatest common measure of 21 and 15. In either case, the pattern of larger entries is LRRL, and therefore, by definition,

$$14 : 10 :: 21 : 15. \tag{3.1}$$

This is not strictly an equation, but an *identity.* The ratio $14 : 10$ is not *equal* to $21 : 15$, but the two ratios are the *same* as one another: they are one. Euclid's language makes the distinction between equality and sameness; the former is not used for ratios.

If we repeat the last letter in LRRL, obtaining LRRLL, and if we replace subsequences of repeated letters with their numbers, we obtain the sequence $(1, 2, 2)$, whose entries appear in the continued fraction

$$1 + \cfrac{1}{2 + \cfrac{1}{2}}.$$

This then is a way to represent the ratio $14 : 10$ or $21 : 15$. We may also note

$$\begin{aligned} 14 &= 2 \cdot 7, & 21 &= 3 \cdot 7, \\ 10 &= 2 \cdot 5, & 15 &= 3 \cdot 5, \end{aligned}$$

where the repetition of the multipliers 7 and 5 is another way to verify the proportion (3.1). However, in this verification, it is important that 7 and 5 are prime to one another, so that they are uniquely determined by either of the pairs $(14, 10)$ and $(21, 15)$, in the sense of being the *least* numbers having the same ratio. It will be a consequence of commutativity that

$$14 \cdot 15 = 21 \cdot 10, \tag{3.2}$$

that is, $(2 \cdot 7) \cdot (3 \cdot 5) = (3 \cdot 7) \cdot (2 \cdot 5)$. Nevertheless, in Euclidean mathematics, an equation like (3.2) cannot serve as a *definition* the proportion (3.1), simply because the equation does not immediately establish that something about the pair $(14, 10)$ is the *same* as for $(21, 15)$.

3.5 Commutativity

Multiplication is certainly commutative in one special case. If one of two factors is unity, then their product is simply the other factor, regardless of which factor is counted as multiplicand.

From the definition of proportionality, all ratios of the form $x : x \cdot a$ are the same. In saying this so compactly, we follow the convention established by Descartes [17], whereby letters from the beginning of the alphabet denote constants, and from the end, variables. All such ratios are the same, since the Euclidean Algorithm, starting with $(x, x \cdot a)$ as the first step, takes a steps, the last being (x, x), and at each step but the last, the right-hand number is greater.

Since also the ratio $1 : 1 \cdot a$ is just $1 : a$, we can conclude

$$1 : a :: b : b \cdot a. \tag{3.3}$$

Suppose now $a : b :: c : d$, so that the steps of the Euclidean algorithm are the same, whether applied to (a, b) or to (c, d). These steps are then the same as for $(a+c, b+d)$, by what we call the commutativity of addition. For, assuming $a > b$, we must also have $c > d$, and so $a + c > b + d$, and consequently

$$(a + c) - (b + d) = (a - b) + (c - d).$$

We conclude

$$a : b :: c : d \text{ implies } a : b :: a + c : b + d. \tag{3.4}$$

As a special case, since $a : b :: a : b$, we have $a : b :: a \cdot 2 : b \cdot 2$. Likewise, repeated application of the implication (3.4) gives

$$a : b :: a \cdot c : b \cdot c.$$

As a special case, $1 : b :: 1 \cdot c : b \cdot c$, that is, $1 : b :: c : b \cdot c$; with different letters,

$$1 : a :: b : a \cdot b.$$

Combining this with (3.3) yields

$$b : a \cdot b :: b : b \cdot a.$$

From this we conclude

$$a \cdot b = b \cdot a.$$

In modern symbolism and typography, such is Euclid's rigorous proof of Proposition 16 of Book VII of the *Elements.* In short, multiplication of numbers is commutative.

3.6 Congruence

Let us henceforth employ the terminology and notation of Gauss, born 1777, who writes at the beginning of the *Disquisitiones Arithmeticae* of 1801 [31],

> Si numerus a numerorum b, c differantiam metitur. b et c *secundum a congrui* dicuntur, sin minus, *incongrui:* ipsum a *modulum* appellamus. Uterque numerorum b, c priori in casu alterius *residuum,* in posteriori vero *nonresiduum* vocatur . . .
>
> Omnia numeri dati a residua secundum modulum m sub formula $a + km$ comprehenduntur, designante k numerum integrum indeterminatum . . .
>
> Numerorum congruentiam hoc signo, $\equiv$, in posterum denotabimus, modulum ubi opus erit in clausulis adiungentes, $-16 \equiv 9$ (mod. 5), $-7 \equiv 15$ (mod. 11).

In the English version of Arthur A. Clarke [32], Gauss's words are rendered as follows.

> If a number a divides the difference of the numbers b and c, b and c are said to be *congruent relative to a*; if not, b and c are *noncongruent.* The number a is called the *modulus.* If the numbers b and c are congruent, each of them is called a *residue* of the other. If they are noncongruent they are called *nonresidues* . . .
>
> Given a, all its residues modulo m are contained in the formula $a + km$ where k is an arbitrary integer . . .
>
> Henceforth we shall designate congruences by the symbol $\equiv$, joining to it in parentheses the modulus when it is necessary to do so; e. g. $-7 \equiv 15$ (mod. 11), $-16 \equiv 9$ (mod. 5).

It would be more faithful to Gauss, and to his predecessors Euclid and Fermat (whom we shall consider presently), to say "measures" where Clarke says "divides." However, we have shown that there is no mathematical difference.

The Latin noun *modulus -i* is the diminutive of *modus -i* "measure." The adjective *secundus -a -um* is the ultimate origin of the English "second," which serves as the ordinal form of the cardinal number "two." In Latin, the form *secundum* serves as a preposition. Where Gauss has *secundum modulum,* meaning something like "following to the [little] measure," Clarke has "modulo." In Latin, *modulo* is the ablative or dative case of *modulus.*

In *An Adventurer's Guide to Number Theory* [29, p. 116], after discussing the congruences $5 \equiv 12 \equiv 1083 \pmod 7$, Richard Friedberg writes,

> If you have studied Latin, you will understand that "modulo 7" is an ablative absolute and means "7 being the modulus." In the eighteenth century, when congruences were first studied, most mathematical articles were written in Latin. The phrase, "modulo 7," was so catchy that it still sticks.

Friedberg is probably correct that *modulo* is in the ablative case; he appears to be wrong about the reason, since our "modulo 7" corresponds to Gauss's *secundum modulum* 7. Probably *modulo* should be understood as an *instrumental* ablative. The uses of the earlier Indo-European instrumental case were apparently taken up by the Latin ablative. In the present context, the modulus is the instrument—the measuring stick—whereby congruence is to be determined.

The *Oxford English Dictionary* [48] traces the number-theoretic use of "modulus" to the 1892 *Theory of Numbers* [44, p. 7] of G. B. Mathews, who more or less repeats Gauss:

> If the difference of two integers b and c is divisible by m, b and c are said to be congruent (or congruous) with respect

> to the modulus m, and this is expressed in writing by
>
> $$b \equiv c \pmod{m}.$$
>
> This is clearly the same thing as $c \equiv b \pmod{m}$. Each of the numbers b, c is said to be a residue (mod m) of the other. With respect to a given modulus, every number b has an infinite number of residues which are included in the expression $b + \lambda m$, λ being any integer.

Thus Mathews avoids any Latin case-forms (as well as absolute constructions).

In *Number Theory and Its History* [50, p. 211], after defining things as Gauss does, Oystein Ore writes simply,

> These terms, as one sees, are derived from Latin, *congruent* meaning *agreeing* or *corresponding* while *modulus* signifies *little measure.*

We can say more. Congruence is originally a geometric notion. Where Heath [21] translates one of Euclid's common notions as

> Things which coincide with one another are equal to one another,

the verb "coincide" might just as well be "are congruent." Euclid's Greek is

τὰ ἐφαρμόζοντα ἐπ' ἀλλήλα ἴσα ἀλλήλοις ἐστίν,

and for Euclid's neuter plural participle *τὰ ἐφαρμόζοντα* (from *ἐπί* + *ἁρμόζω*, the latter being related to *ἡ ἁρμονία* and thus to our "harmony"), Commandinus [19] and Heiberg [20] use the Latin source of our adjective "congruent," thus:

quę sibi ipsis congruunt, inter se sunt ęqualia.
quae inter se congruunt, aequalia sunt.
τὰ ἐφαρμόζοντα ἐπ' ἀλλήλα ἴσα ἀλλήλοις ἐστίν.

(Commandinus's printer uses the ę or *e caudata* for *ae*. The printer uses also the old-fashioned long ess, when the ess is not terminal, but I have not managed to print this with LaTeX.)

3.7 Divisibility

We are now allowed to use the notions of division and measurement interchangeably. We may also consider our objects of study to be not simply counting numbers, but "signed" counting numbers, or *integers*—of which the counting numbers are just the positive instances.

Thus for example the Euclidean Algorithm allows us to find what is now called the *greatest common divisor* or "gee cee dee" (gcd) of two numbers. Moreover, the Algorithm allows us to solve the equation

$$ax + by = \gcd(a, b),$$

where now one of x and y will be negative when a and b are positive. This result is called **Bézout's Lemma,** perhaps by way of impressing on students the importance of the result; such possibilities are discussed in "The Theorem of Thales: A Study of the Naming of Theorems in School Geometry Textbooks" [51], a source I used in my own study of Thales's Theorem [54]. The connection of Bézout to the lemma named for him does seem even more tenuous than in the case of Thales.

To symbolize that an integer a measures or divides an integer b, we may write

$$a \mid b.$$

I do not know the origin of this notation, but Landau used it in 1927 [40, p. 11], and Hardy and Wright (who also use it) say in 1938 [33, p. vii],

> To Landau in particular we, in common with all serious students of the theory of numbers, owe a debt which we could hardly overstate.

For Landau and for Hardy and Wright, unlike Gauss, the symbolism of divisibility comes before that of congruence. Hardy and Wright [33, p. 49] observe of congruence,

> The definition does not introduce any new idea, since '$x \equiv a \pmod{m}$' and '$m \mid x - a$' have the same meaning, but each notation has its advantages.

Strictly speaking, Landau's sign of divisibility is oblique, like the solidus we use for denoting fractions. For us, a/b is a rational number; for Landau, it is the assertion that $aq = b$ for some integer q. This assertion has the consequence that Landau expresses as $|a|/|b|$; we have to write, more confusingly, $|a| \mid |b|$. However, there are no other absolute values discussed in the present work.

The fraction that for us is a/b is for Landau $\frac{a}{b}$ or $a : b$. It so happens that Landau finds greatest common divisors, not with the Euclidean Algorithm, but by first observing that the least common multiple of a and b divides every common multiple (since otherwise the remainder would be a common multiple less than the least).

The quotient of ab by the least common multiple of a and b is shown to be the greatest common divisor. Landau and Hardy and Wright denote this by (a, b), which is convenient for international use; but I shall stick with $\gcd(a, b)$. Hardy and Wright also use $\{a, b\}$, with braces, to denote the least common multiple of a and b; but I shall use $\operatorname{lcm}(a, b)$. Thus

$$\frac{ab}{\operatorname{lcm}(a,b)} \cdot \frac{\operatorname{lcm}(a,b)}{b} = a,$$

and similarly with a and b interchanged, so $ab/\operatorname{lcm}(a, b)$ is a common divisor of a and b. If d is a common divisor, then ab/d is a common multiple, so

$$\operatorname{lcm}(a,b) \;\Big|\; \frac{ab}{d}, \qquad\qquad d \;\Big|\; \frac{ab}{\operatorname{lcm}(a,b)}.$$

Thus

$$\gcd(a,b) = \frac{ab}{\operatorname{lcm}(a,b)}. \tag{3.5}$$

We shall use this and its notation once later. We shall have used braces as is customary today, to delineate sets.

If $a \mid bc$ and $\gcd(a, b) = 1$, then, since ab is the least common multiple of a and b, and bc is *some* common multiple, we have $ab \mid bc$ by what we have shown. It now follows that $a \mid c$. This is Landau's proof of what we shall call **Euclid's Lemma.** Strictly, Proposition 30 of Book VII of the *Elements* is the case where a is prime.

Bézout's Lemma gives the neat proof of Euclid's Lemma that may be more common than Landau's. From $ax + by = 1$, we obtain $acx + bcy = c$, so that, since $a \mid acx$, if also $a \mid bc$, we can conclude $a \mid c$.

Useful for us at present is indeed Euclid's special case. With respect to a prime modulus p, if $ab \not\equiv 0$, then neither of a and b can be congruent to 0. This gives us **cancellation:** if $a \not\equiv 0$, and $ab \equiv ac$, then $b \equiv c$. Thus the first $p - 1$ multiples of a, starting from a itself, are incongruent to one another and to 0.

Any list of numbers with this property can have length at most $p-1$. Thus if we add the number 1 to the list of multiples of a, it must be congruent to one of these multiples. This means a is **invertible** with respect to p. With the Euclidean Algorithm, we can actually find the inverse, since $ax+py=1$ means $ax \equiv 1 \pmod{p}$.

3.8 Fermat's Theorem

On Thursday, October 18, 1640, in a letter to Bernard Frénicle de Bessy (1605–1675), Pierre de Fermat (1601–65) described as follows what we now know as **Fermat's Theorem** [24, p. 209].

> Tout nombre premier mesure infailliblement une des puissances − 1 de quelque progression que se soit, et l'exposant de la dite puissance est sous-multiple du nombre premier donné − 1; et, après qu'on a trouvé la première puissance qui satisfait à la question, toutes celles dont les exposants sont multiples de l'exposant de la première satisfont tout de même à la question.
>
> Exemple: soit la progression donnée
>
> | | | | | | | |
> |---|---|---|---|---|---|---|
> | 1 | 2 | 3 | 4 | 5 | 6 | |
> | 3 | 9 | 27 | 81 | 243 | 729 | etc. |
>
> avec ses exposants en dessus.
>
> Prenez, par exemple, le nombre premier 13. Il mesure la troisième puissance − 1, de laquelle 3, exposant, est sous-multiple de 12, qui est moindre de l'unité que le nombre 13, et parce que l'exposant de 729, qui est 6, est multiple du premier exposant, qui est 3, il s'ensuit que 13 mesure aussi lat dite puissance 729 − 1.

> Et cette proposition est généralement vraie en toutes progressions et en tous nombres premiers; de quoi je vous envoierois la démonstration, si je n'appréhendois d'être trop long.

In his *Source Book in Mathematics, 1200–1800* [25, p. 28], Struik translates Fermat as below. Instead of *measures,* Struik says "is a factor of"; instead of *submultiple,* "divisor." He also misdates the letter as being of October 10, 1640.

> Every prime number is always a factor [*mesure infailliblement*] of one of the powers of any progression minus 1, and the exponent of this power is a divisor of the prime number minus 1. After one has found the first power that satisfies the proposition, all those powers of which the exponents are multiples of the exponent of the first power also satisfy the proposition.
>
> *Example:* Let the given progression be
>
> $$\begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & \\ 3 & 9 & 27 & 81 & 243 & 729 & \text{etc.} \end{array}$$
>
> with its exponents written on top.
>
> Now take, for instance, the prime number 13. It is a factor of the third power minus 1, of which 3 is the exponent and a divisor of 12, which is one less than the number 13, and because the exponent of 729, which is 6, is a multiple of the first exponent, which is 3, it follows that 13 is also a factor of this power 729 minus 1.
>
> And this proposition is generally true for all progressions and for all prime numbers, of which I would send you the proof if I were not afraid to be too long.

According to Fermat then, for every number a, for every prime number p, there is a positive exponent ℓ such that, with respect to the modulus p,

$$a^\ell \equiv 1;$$

moreover, if k is the least such ℓ, then $k \mid p-1$ and $a^{kx} \equiv 1$ (for every multiplier x). Let us not fault Fermat for omitting the condition $a \not\equiv 0$ and for not strictly observing that, conversely, k divides every ℓ.

Usually what is called **Fermat's Theorem** is the special case that $a^{p-1} \equiv 1$ when $p \nmid a$. This is the usage of Gauss, who derives the result after proving the above result $k \mid p-1$. He then observes that one can prove the basic form of Fermat's Theorem by induction. Indeed, the claim is trivially true when $a = 1$. If it is true when $a = b$, then it is true when $a = b+1$, since, as a consequence of Euclid's Lemma,

$$(b+1)^p \equiv b^p + 1 \pmod{p}.$$

Gauss attributes this proof to Euler.

Gauss also attributes to Euler a proof of the more general assertion of Fermat. We can summarize the proof as follows, using the terminology of Landau [40, p. 42], whereby, with respect to a modulus n, a **complete set of residues** has any two, and therefore all three, of the following properties:

1) there are exactly n members of the set,
2) no two members are congruent,
3) every number is congruent to one of them.

If from a complete set of residues we select precisely those members that are prime to n, we have a **reduced set of residues.** For any prime number p and any a that is prime to p, there must be numbers b_i such that the entries in the table below are incongruent to one another and compose a reduced set of residues with respect to p.

$$\begin{array}{cccc}
a & a^2 & \cdots & a^k \\
ab_1 & a^2b_1 & \cdots & a^kb_1 \\
ab_2 & a^2b_2 & \cdots & a^kb_2 \\
\multicolumn{4}{c}{\dotfill} \\
ab_n & a^2b_n & \cdots & a^kb_n
\end{array}$$

In particular, the table has k columns and $p-1$ entries, and therefore $k \mid p-1$.

3.9 Algebra

Since a reduced set of residues with respect to a given modulus is closed under both multiplication and inversion, those residues compose a finite **group.** If the modulus is n, then the size of the group of reduced residues is the number recognized by Euler and denoted by Gauss by

$$\varphi(n).$$

(Actually Gauss just wrote ϕn.)

The general form of Fermat's Theorem is then a special case of the **Lagrange Theorem,** which is that the order of a finite group is divisible by the order of every subgroup. Relevant sections of Lagrange's paper [38] are selected and translated in Struik's *Source Book* [39]; but as far as I can tell, one can infer from the paper only that the "Lagrange Theorem" holds when the group is the group of permutations of finitely many objects.

Abstract algebra both illuminates and complicates the number theory or *arithmetic* that is its origin. Number theory involves various structures, such as the groups of residues just mentioned; algebra looks at these as wholes and gives them names.

As being ordered and being capable of being added and multiplied as learned in school, the integers compose a so-called *ordered commutative ring,* denoted by $\mathbb{Z}$, supposedly for the German Zahl. If we are going to use the symbol $\mathbb{Z}$, we might as well also allow the symbol $\mathbb{N}$ for the positive part of $\mathbb{Z}$, consisting of the counting numbers.

One sometimes wants a name for the *non-negative* part of $\mathbb{Z}$, namely the positive part with zero. Some writers use $\mathbb{N}$ for this part, but the name ω (omega) is already used in set theory, and so I would use that, if I had a need, which I do not in the present work.

Landau and Hardy and Wright do not need even a symbol like $\mathbb{Z}$. The term "ring" for what is symbolized by $\mathbb{Z}$ may be unfortunate, but it seems to arise from the observation that, for example, the real numbers $a + b\surd 2$, where a and b are integers, also compose a ring, since the product of two such numbers "circles back" to being such a number as well:

$$(a + b\surd 2)(c + d\surd 2) = ac + 2bd + (ad + bc)\surd 2.$$

Given n in $\mathbb{N}$, for the moment we let

$$[a]_n = \{x \colon x \equiv a\} \pmod{n},$$

the **congruence class** of a with respect to n. We use this only to define

$$\mathbb{Z}_n = \{[x]_n \colon x \in \mathbb{Z}\},$$

the set of congruence classes with respect to n. Here we are only replacing each element of a complete set of residues with its congruence class. Like $\mathbb{Z}$ itself, $\mathbb{Z}_n$ is a commutative ring, though it is not ordered.

The multiplicatively invertible elements—the **units**—of $\mathbb{Z}_n$ compose the group denoted by

$$\mathbb{Z}_n{}^{\times}.$$

Again, the size or **order** of this group is $\varphi(n)$. For every prime p, since $\varphi(p) = p - 1$, this means both that $\mathbb{Z}_p$ is a **field**—a commutative ring, like the ring of rational or real numbers, in which every nonzero element is invertible—and that (with the help of the Lagrange Theorem) Fermat's Theorem holds.

3.10 Primitive roots

If d and n are counting numbers, d dividing n, then the integers that have with n the greatest common divisor d are in one-to-one correspondence with the integers that are prime to n/d. The correspondence is between dx and x, where $\gcd(x, n/d) = 1$. Moreover, for every element a of $\mathbb{Z}_n$, $\gcd(a, n)$ is well-defined, and it divides n. In symbols then, for all a in $\mathbb{Z}_n$,

$$\gcd(a, n) = d \text{ if and only if } d \mid a \;\;\&\;\; \gcd\left(\frac{a}{d}, \frac{n}{d}\right) = 1. \quad (3.6)$$

This conclusion will serve as a lemma for a theorem that Gauss sets out [31, ¶39], as we shall, in Euclid's *protasis* style. I take the terminology here from David Fowler [28, p. 386], as naming the style's "distinctive and useful opening feature, the enunciation or *protasis*." In a proposition of Euclid, first comes an enunciation, and only then comes the demonstration or proof of what has been enunciated. Students readily adopt this style, first writing what they want to prove, then writing down more things, which they hope will be considered as a proof. It is not always clear that the students understand the logical relations involved.

Euclid avoids confusing his readers by following a consistent pattern. Each of his propositions has up to six parts, always in the same order. In his commentary on Euclid, Proclus names the parts of a proposition as enunciation (*πρότασις*), exposition, specification, construction, demonstration, and conclusion [59, p. 159 (203)].

Neither Proclus nor Euclid has a name for what we call the proposition as a whole. Proclus says, in Morrow's translation [59, p. 63 (77)],

> Again the propositions that follow from the first principles he divides into problems and theorems;

but as in the King James Bible [7, p. 323], the words "propositions that follow" could be italicized, as having no explicit counterpart in the Greek, which, for the passage just quoted, is [58, p. 77]

> *Πάλιν δ' αὖ τὰ ἀπὸ τῶν ἀρχῶν εἰς προβλήματα διαιρεῖται καὶ θεωρήματα.*

Pappus makes the etymology clear [65, pp. 566 f.]: in a problem (*πρόβλημα*) it is proposed (*προβάλλεταί*) to do something; in a theorem (*θεώρημα*), the implications of hypotheses are contemplated (*θεωρεῖται*). Euclid signals the distinction between a problem and a theorem by how he ends it, using respectively the words that we translate into Latin and abbreviate as Q.E.F. ("which was to be done") and Q.E.D. ("which was to be proved").

A web edition of Euclid's Greek text labels each proposition as a *πρότασις* [22]. This conforms to the modern practice of treating the enunciation as a *metonym* for the proposition as a whole. Here the terminology is from Reviel Netz, who argues that for Euclid the *diagram* is the metonym of the proposition [49, p. 38]. The handy little book called *The Bones* [23] does not choose sides, but supplies both the enunciation and the diagram (and nothing else) for each of Euclid's propositions.

For the proposition below, Gauss simply italicizes his protasis:

> *Si a, a′, a″, etc. sunt omnes divisores ipsius A (unitate et ipso A non exclusis), erit*
>
> $$\phi a + \phi a' + \phi a'' + \textit{etc.} = A.$$

We give the protasis a bold label.

Theorem (Gauss). *The sum of the values of* $\varphi(d)$*, as* d *ranges over the positive divisors of* n*, is just* n *itself; in symbols,*

$$\sum_{d|n} \varphi(d) = n. \tag{3.7}$$

Proof. Suppose $d \mid n$. By (3.6), the two sets

$$\{x \in \mathbb{Z}_n \colon \gcd(x, n) = d\}, \quad \{y \in \mathbb{Z}_{n/d} \colon \gcd(y, n/d) = 1\}$$

have the same size. The size of the latter set being $\varphi(n/d)$, we can conclude

$$n = \sum_{d|n} \varphi\left(\frac{n}{d}\right).$$

This yields (3.7), by symmetry. □

The **order** of an element a of $\mathbb{Z}_n{}^{\times}$ is the least positive exponent ℓ such that $a^{\ell} = 1$. In symbols,

$$\operatorname{ord}_n(a) = \min\{x \in \mathbb{N} \colon a^x = 1\}.$$

If we think of a as an integer, rather than a congruence class, we should perhaps write something like

$$\operatorname{ord}_n(a) = \min\{x \in \mathbb{N} \colon a^x \equiv 1\} \pmod{n}.$$

If it exists, a **primitive root** of n is an element of $\mathbb{Z}_n{}^\times$ having order $\varphi(n)$. Euler gave a proof of the following, but there was a gap, which, according to Burton [6, p. 162], Legendre filled. Gauss mentions the gap, but does not mention Legendre.

Theorem. *Every prime number has a primitive root.*

Proof. Let p be a prime number. We shall show that the number of its primitive roots is $\varphi(p-1)$, which is positive. Since $\varphi(p) = p-1$, the order of every element of $\mathbb{Z}_p{}^\times$ measures this. If $d \mid p-1$, let us denote by

$$\psi_p(d)$$

the number of elements of $\mathbb{Z}_p{}^\times$ having order d. We want to show $\psi_p(d) \geqslant 1$. Since every element of $\mathbb{Z}_p{}^\times$ has some such order d, we have

$$p - 1 = \sum_{d \mid p-1} \psi_p(d).$$

If we can show $\psi_p(d) \leqslant \varphi(d)$, then, by the previous theorem, we must have $\psi_p(d) = \varphi(d)$, which is positive, and so we shall be done.

Suppose then $\psi_p(d) > 0$, so that some a in $\mathbb{Z}_p{}^\times$ has order d. The d elements of the set $\{a^t \colon t \in \mathbb{Z}_d\}$ are solutions of the congruence

$$x^d \equiv 1 \pmod{p}.$$

They must be the only solutions, since the congruence can have at most d solutions (since $\mathbb{Z}_p$ is a field). Therefore, with respect to $p-1$,

$$\begin{aligned}\operatorname{ord}_p(a^k) &= \min\{x \in \mathbb{N}\colon a^{kx} \equiv 1\} \\ &= \frac{1}{k}\min\{y \in \mathbb{N}\colon k \mid y \ \ \&\ \ a^y \equiv 1\} \\ &= \frac{1}{k}\min\{y \in \mathbb{N}\colon k \mid y \ \ \&\ \ d \mid y\} \\ &= \frac{\operatorname{lcm}(k,d)}{k},\end{aligned}$$

and this is $d/\gcd(k,d)$, by (3.5) on page 68. Thus, if it is positive, $\psi_p(d)$ must be the size of the set

$$\{x \in \mathbb{Z}_d\colon \gcd(x,d)=1\},$$

and this size is by definition $\varphi(d)$. □

The foregoing is the *first* of Gauss's two proofs. It is the one that Hardy and Wright give [33, pp. 85 f.]; but they give it, unlike Gauss, *after* proving Gauss's Law of Quadratic Reciprocity. Like other writers, they follow Gauss in using the notation ψ where I have ψ_p. It seems to me desirable to use the subscript p, so that the ultimate independence of $\psi_p(d)$ from p (as long as $d \mid p-1$) may be all the more remarkable. I also make the subtle distinction of using an upright letter ψ for something defined once for all; an italic letter like ψ may have different meanings in different settings, even though the meaning may be considered constant in a particular setting.

3.11 Two more proofs

Landau gives Gauss's second proof that primes have primitive roots, but he too gives it, like Hardy and Wright, only after

Quadratic Reciprocity. It uses the Fundamental Theorem of Arithmetic, that every prime number has a unique prime factorization. Gauss seems to have been the first person to state this explicitly [33, p. 10].

Briefly, suppose $p-1$ has the prime factorization $\prod_q q^{d(q)}$. For each prime q in the product, since the congruence

$$x^{(p-1)/q} \equiv 1 \pmod{p}$$

has at most $(p-1)/q$ solutions, it has a non-solution, a_q, from ${\mathbb{Z}_p}^{\times}$. Then $q^{d(q)}$ is the order of the power

$${a_q}^{(p-1)/q^{d(q)}},$$

and the product $\prod_q {a_q}^{(p-1)/q^{d(q)}}$ of all of these powers has order $p-1$.

For a third proof that every prime number has a primitive root, noting as we have that $\mathbb{Z}_p$ is a field, we can just prove generally that the group of units of every finite field K is *cyclic.* Again briefly, if a and b in $K^{\times}$ have orders k and m, then ab must have order km, if k and m are prime to one another. As a result, if $\gcd(k,m)=d$, then $a^d b$ has order km/d, which is $\operatorname{lcm}(k,m)$. Thus if a already has maximal order, then $k \mid m$. In this case, every element of $K^{\times}$ is a root of the polynomial x^m-1; in a field, by a result that we have already used, this polynomial can have no more than m roots; therefore m is less by 1 than the size of K.

3.12 Practicalities

The number 997 is prime, because (1) it is less than 1024, which is the square of 32, and (2) it is indivisible by the primes less than 32, namely 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, and 31. Now we know that 997 has a primitive root, and Gauss's second proof suggests a procedure for finding one. Alternatively, if a is a candidate, since 996 has the prime factorization $2^2 \cdot 3 \cdot 83$, it is enough to check that none of the powers

$$a^{2^2 \cdot 3}, \qquad a^{2^2 \cdot 83}, \qquad a^{3 \cdot 83}$$

is congruent to unity. One can compute these by hand by taking successive squares and using for example

$$83 = 64 + 16 + 2 + 1 = 2^6 + 2^4 + 2^2 + 2^0.$$

In fact a table of primes and their primitive roots in Burton [6, p. 393] gives 7 as the least primitive root of 997. For the table of antilogarithms in §2.2, I computed a list of exponents and the corresponding powers of 7 *modulo* 997 with an electronic spreadsheet (LibreOffice Calc), relying on the rule

$$k^2 \equiv \ell \text{ implies } (k+1)^2 \equiv \ell + 2k + 1.$$

The spreadsheet might then order the list according to the powers, rather than the exponents; but for the table of logarithms in §2.1, I used the MakeIndex program coming with LaTeX to do the reordering.

Bibliography

[1] Dawn Ades, Neil Cox, and David Hopkins. *Marcel Duchamp*. World of Art. Thames and Hudson, London, 1999.

[2] Liz Erçevik Amado, editor. *Anne, ben barbar miyim? / Mom, am I a barbarian?* Istanbul Foundation for Culture and Arts, 2013. 13th Istanbul Biennial Guide.

[3] Isaac Asimov. *An Easy Introduction to the Slide Rule*. Fawcett, Greenwich, Conn., 1967. First published by Houghton Mifflin, 1965.

[4] William Blake. *The Marriage of Heaven and Hell*. Oxford University Press, 1985. Facsimile edition, first published in 1975, with introduction and commentary by Sir Geoffrey Keynes.

[5] Alexandre Borovik. Metamathematics of elementary mathematics. `www.matematikdunyasi.org/yazokulu/borovik_1b.pdf`, July 2008. Lecture at the Nesin Mathematics Village, Şirince, Selçuk, Izmir, Turkey.

[6] David M. Burton. *Elementary Number Theory*. McGraw-Hill, Boston, sixth edition, 2007.

[7] Robert Carroll and Stephen Prickett, editors. *The Bible: Authorized King James Version with Apocrypha*. Oxford World's Classics. Oxford, 2008. First published 1997.

[8] Claude Closky. The first thousand numbers classified in alphabetical order. `www.ubu.com/concept/closky_1000.html`, accessed November 29, 2017, 1989.

[9] R. G. Collingwood. *Religion and Philosophy.* Macmillan, London, 1916. `archive.org/details/religionphilosop00colliala`, accessed November 21, 2016.

[10] R. G. Collingwood. *Speculum Mentis or The Map of Knowledge.* Clarendon Press, Oxford, 1924. Reprinted photographically in Great Britain at the University Press, Oxford, 1946.

[11] R. G. Collingwood. *The Principles of Art.* Clarendon Press, Oxford, 1938. Issued as an Oxford University Press paperback 1958.

[12] R. G. Collingwood. *An Autobiography.* Clarendon Press, Oxford, 1978. First published 1939. With a new introduction by Stephen Toulmin. Reprinted 2002.

[13] R. G. Collingwood. *The New Leviathan, or Man, Society, Civilization, and Barbarism.* Clarendon Press, revised edition, 2000. With an Introduction and additional material edited by David Boucher. First edition 1942.

[14] R. G. Collingwood. *An Essay on Philosophical Method.* Clarendon Press, Oxford, new edition, 2005. With an Introduction and additional material edited by James Connelly and Giuseppina D'Oro. First edition 1933.

[15] Arthur C. Danto. *What Art Is.* Yale University Press, New Haven, 2013.

[16] Richard Dedekind. *Essays on the Theory of Numbers. I: Continuity and Irrational Numbers. II: The Nature and Meaning of Numbers.* Dover Publications, New York, 1963. Authorized 1901 translation by Wooster Woodruff Beman of "Stetigkeit und irrationale Zahlen" and "Was sind und was sollen die Zahlen" (second edition, 1893; first, 1887).

[17] René Descartes. *La Géométrie.* Jacques Gabay, Sceaux, France, 1991. Reprint of Hermann edition of 1886.

[18] John Donne. *The Complete Poetry and Selected Prose of John Donne.* The Modern Library, New York, 1952. Edited with an introduction by Charles M. Coffin.

[19] Euclid. *Euclidis Elementorum Libri XV.* Jacobus Chriegher, Pisauri (Pesaro), 1572. Latin version by Federico Commandino. Digitized by Google. `www.wilbourhall.org/`, accessed November 24, 2017.

[20] Euclid. *Euclidis Elementa*, volume I of *Euclidis Opera Omnia.* Teubner, Leipzig, 1883. Edited with Latin interpretation by I. L. Heiberg. Books I–IV.

[21] Euclid. *The Thirteen Books of Euclid's* Elements. Dover Publications, New York, 1956. Translated from the text of Heiberg with introduction and commentary by Thomas L. Heath. In three volumes. Republication of the second edition of 1925. First edition 1908.

[22] Euclid. *Στοιχεία Ευκλείδου.* `users.ntua.gr/dimour/euclid/`, 1999. Edited by Dimitrios E. Mourmouras. Accessed December 24, 2014.

[23] Euclid. *The Bones: A handy where-to-find-it pocket reference companion to Euclid's* Elements. Green Lion Press, Santa Fe, NM, 2002. Conceived, designed, and edited by Dana Densmore.

[24] Pierre de Fermat. *Oeuvres de Fermat. Tome Deuxième. Correspondance.* Gautiers-Villars et Fils, Paris, 1894. Edited by Paul Tannery and Charles Henry. `archive.org/details/oeuvresdefermat02ferm`, accessed November 23, 2017.

[25] Pierre de Fermat. Letter to Bernard Frénicle de Bessy, October 18, 1640. In Struik [64], pages 27–29. Reprint of the 1969 edition.

[26] Richard P. Feynman. *"Surely You're Joking, Mr. Feynman!"*. W.W. Norton & Company, New York and London, 1985. Adventures of a Curious Character; as told to Ralph Leighton; edited by Edward Hutchings.

[27] David Fowler. Dedekind's theorem: $\sqrt{2} \times \sqrt{3} = \sqrt{6}$. *Amer. Math. Monthly*, 99(8):725–733, 1992.

[28] David Fowler. *The Mathematics of Plato's Academy: A new reconstruction*. Clarendon Press, Oxford, second edition, 1999.

[29] Richard Friedberg. *An Adventurer's Guide to Number Theory*. Dover, New York, 1994. Corrected and expanded reprint of the 1968 original.

[30] Robert Frost. *Selected Poems of Robert Frost*. Holt, Rinehart and Winston, New York, 1963. Introduction by Robert Graves.

[31] Carl Friedrich Gauss. *Disquisitiones Arithmeticae*. Carl Friedrich Gauss Werke. Gerh. Fleischer Jun., Leipzig, 1801. Electronic version of the original Latin text from Goettingen State and University Library.

[32] Carl Friedrich Gauss. *Disquisitiones Arithmeticae*. Springer-Verlag, New York, 1986. Translated into English by Arthur A. Clarke, revised by William C. Waterhouse.

[33] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. Clarendon Press, Oxford, fifth edition, 1979. First edition 1938. Reprinted 1990.

[34] David Hilbert. *The Foundations of Geometry*. Authorized translation by E. J. Townsend. Reprint edition. The Open

Court Publishing Co., La Salle, Ill., 1959. Based on lectures 1898–99. Translation copyrighted 1902. Project Gutenberg edition released December 23, 2005 (`www.gutenberg.net`).

[35] Jens Hoffmann and Adriano Pedrosa, editors. *İsimsiz (12. İstanbul Bienali) / Untitled (12th Istanbul Biennial)*. Istanbul Foundation for Culture and Arts, 2011.

[36] Julian Jaynes. *The Origin of Consciousness in the Breakdown of the Bicameral Mind*. Houghton Mifflin, Boston, 1977.

[37] J. P. Kenyon, editor. *The Wordsworth Dictionary of British History*. Wordsworth Reference, Ware, Hertfordshire, 1994. Foreword by Norman Stone.

[38] Joseph Louis Lagrange. Suite des réflexions sur la résolution algébrique des équations. In *Nouveaux Mémoires de L'Académie Royale des Sciences et Belles-Lettres. Année MDCCLXXI*. Chrétien Fréderic Voss, Berlin, 1773.

[39] Joseph Louis Lagrange. On the general theory of equations. In Struik [64], pages 102–11. Reprint of the 1969 edition.

[40] Edmund Landau. *Elementary Number Theory*. Chelsea Publishing, New York, 1958. Originally part of *Vorlesungen über Zahlentheorie* (Leipzig, 1927). Translated by J. E. Goodman.

[41] Geoffrey Lewis. *Turkish Grammar*. Oxford University Press, second edition, 2000. First edition 1967.

[42] Henry George Liddell and Robert Scott. *A Greek-English Lexicon*. Clarendon Press, Oxford, 1996. "Revised and augmented throughout by Sir Henry Stuart Jones, with the assistance of Roderick McKenzie and with the cooperation of many scholars. With a revised supplement." First edition 1843; ninth edition 1940.

[43] David Macauley. *Cathedral: The Story of Its Construction*. Houghton Mifflin, Boston, 1973.

[44] G. B. Mathews. *Theory of Numbers*. Chelsea, New York, second edition, no date.

[45] Mary Midgley. *Evolution as a Religion*. Routledge, London and New York, revised edition, 2002. With a new introduction by the author. First published 1985.

[46] Mary Midgley. *Heart and Mind: The Varieties of Moral Experience*. Routledge, London, 2003. First published 1981. With a new introduction by the author.

[47] Mary Midgley. The golden age of female philosophy. *The Guardian*, 28 November 2013.

[48] James A. H. Murray et al., editors. *The Compact Edition of the Oxford English Dictionary*. Oxford University Press, 1971. Complete text reproduced micrographically. Two volumes. Original publication, 1884–1928.

[49] Reviel Netz. *The Shaping of Deduction in Greek Mathematics*, volume 51 of *Ideas in Context*. Cambridge University Press, Cambridge, 1999. A study in cognitive history.

[50] Oystein Ore. *Number Theory and Its History*. Dover, New York, 1988. Reprint of the 1948 original, With a supplement.

[51] Dimitris Patsopoulos and Tasos Patronis. The theorem of Thales: A study of the naming of theorems in school geometry textbooks. *The International Journal for the History of Mathematics Education*, 1(1), 2006. `www.comap.com/historyjournal/index.html`, accessed September 2016.

[52] David Pierce. St John's College. *The De Morgan Journal*, 2(2):62–72, 2012. `education.lms.ac.uk/wp-content/`

uploads/2012/02/st-johns-college.pdf, accessed October 1, 2014.

[53] David Pierce. Abscissas and ordinates. *J. Humanist. Math.*, 5(1):223–264, 2015. scholarship.claremont.edu/jhm/vol5/iss1/14.

[54] David Pierce. Thales and the nine-point conic. *The De Morgan Gazette*, 8(4):27–78, 2016. education.lms.ac.uk/2016/12/thales-and-the-nine-point-conic/, accessed June 1, 2017.

[55] David Pierce. On commensurability and symmetry. *J. Humanist. Math.*, 7(2):90–148, 2017. scholarship.claremont.edu/jhm/vol7/iss2/6.

[56] Robert M. Pirsig. *Lila*. Bantam, New York, 1992.

[57] Robert M. Pirsig. *Zen and the Art of Motorcycle Maintenance*. William Morrow, New York, 1999. Twenty-fifth Anniversary Edition. With a new introduction by the author.

[58] Proclus. *Procli Diadochi in Primum Euclidis Elementorum Librum Commentarii*. Bibliotheca scriptorum Graecorum et Romanorum Teubneriana. In aedibus B. G. Teubneri, 1873. Ex recognitione Godofredi Friedlein.

[59] Proclus. *A Commentary on the First Book of Euclid's* Elements. Princeton Paperbacks. Princeton University Press, Princeton, NJ, 1992. Translated from the Greek and with an introduction and notes by Glenn R. Morrow. Reprint of the 1970 edition. With a foreword by Ian Mueller.

[60] Herbert Read. *A Concise History of Modern Painting*. Thames and Hudson, London, new and augmented edition, 1974. [First edition 1959.] Revised edition 1968. Reprinted 1986.

[61] J. D. Salinger. *Franny and Zooey*. Little, Brown, Boston, 1961.

[62] Joe Shannon. *Representation Abroad.* Smithsonian Institution, Washington, 1985. Dates of exhibition at the Hirshhorn Museum and Sculpture Garden, June 5–September 2, 1985.

[63] Barry Hartley Slater. Aesthetics. In James Fieser and Bradley Dowden, editors, *Internet Encyclopedia of Philosophy.* `www.iep.utm.edu/aestheti/`, accessed November 2, 2017.

[64] D. J. Struik, editor. *A Source Book in Mathematics, 1200–1800.* Princeton Paperbacks. Princeton University Press, Princeton, NJ, 1986. Reprint of the 1969 edition.

[65] Ivor Thomas, editor. *Selections Illustrating the History of Greek Mathematics. Vol. II. From Aristarchus to Pappus.* Number 362 in Loeb Classical Library. Harvard University Press, Cambridge, Mass, 1951. With an English translation by the editor.

[66] Stephen Trombley. *Fifty Thinkers Who Shaped the Modern World.* Atlantic Books, London, 2012.

[67] Arthur W. Weeks and Jackson B. Adkins. *A Course in Geometry: Plane and Solid.* Ginn and Company, Lexington MA, 1970.

[68] Arthur W. Weeks and Jackson B. Adkins. *Second Course in Algebra With Trigonometry.* Ginn and Company, Lexington MA, 1971.

[69] Walt Whitman. *Leaves of Grass and Selected Prose.* Rinehart & Company, New York, 1949. Edited and with an introduction by Sculley Bradley.

[70] Jr. William Strunk and E. B. White. *The Elements of Style.* Macmillan, New York, 1962.