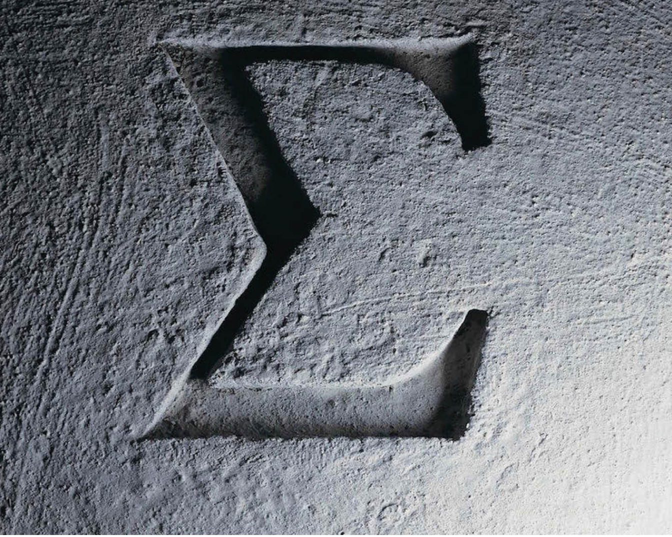
CONCRETE MATHEMATICS

A FOUNDATION FOR COMPUTER SCIENCE

GRAHAM ○ KNUTH ○ PATASHNIK

SECOND EDITION



This page intentionally left blank

CONCRETE MATHEMATICS

Second Edition

Dedicated to Leonhard Euler (1707–1783)

A Foundation for Computer Science

CONCRETE MATHEMATICS

Second Edition

Ronald L. Graham
AT&T Bell Laboratories

Donald E. Knuth
Stanford University

Oren Patashnik
Center for Communications Research

ADDISON–WESLEY
Upper Saddle River, NJ • Boston • Indianapolis • San Francisco
New York • Toronto • Montréal • London • Munich • Paris • Madrid
Capetown • Sydney • Tokyo • Singapore • Mexico City

Library of Congress Cataloging-in-Publication Data

```
Graham, Ronald Lewis, 1935-
    Concrete mathematics : a foundation for computer science / Ronald
  L. Graham, Donald E. Knuth, Oren Patashnik. -- 2nd ed.
  xiii,657 p.  24 cm.
  Bibliography:  p. 604
  Includes index.
  ISBN 978-0-201-55802-9
  1. Mathematics.  2. Computer science-Mathematics.  I. Knuth,
Donald Ervin, 1938-    .  II. Patashnik, Oren, 1954-    .  III. Title.
QA39.2.G733 1994
510-dc20                                                       93-40325
                                                                    CIP
```


Internet page `http://www-cs-faculty.stanford.edu/~knuth/gkp.html` contains current information about this book and related books.

Electronic version by Mathematical Sciences Publishers (MSP), `http://msp.org`

ISBN-13 978-0-201-55802-9
ISBN-10 0-201-55802-5

First digital release, August 2015

Preface

"Audience, level, and treatment — a description of such matters is what prefaces are supposed to be about."
— P. R. Halmos [173]

THIS BOOK IS BASED on a course of the same name that has been taught annually at Stanford University since 1970. About fifty students have taken it each year — juniors and seniors, but mostly graduate students — and alumni of these classes have begun to spawn similar courses elsewhere. Thus the time seems ripe to present the material to a wider audience (including sophomores).

It was a dark and stormy decade when Concrete Mathematics was born. Long-held values were constantly being questioned during those turbulent years; college campuses were hotbeds of controversy. The college curriculum itself was challenged, and mathematics did not escape scrutiny. John Hammersley had just written a thought-provoking article "On the enfeeblement of mathematical skills by 'Modern Mathematics' and by similar soft intellectual trash in schools and universities" [176]; other worried mathematicians [332] even asked, "Can mathematics be saved?" One of the present authors had embarked on a series of books called *The Art of Computer Programming*, and in writing the first volume he (DEK) had found that there were mathematical tools missing from his repertoire; the mathematics he needed for a thorough, well-grounded understanding of computer programs was quite different from what he'd learned as a mathematics major in college. So he introduced a new course, teaching what he wished somebody had taught him.

"People do acquire a little brief authority by equipping themselves with jargon: they can pontificate and air a superficial expertise. But what we should ask of educated mathematicians is not what they can speechify about, nor even what they know about the existing corpus of mathematical knowledge, but rather what can they now do with their learning and whether they can actually solve mathematical problems arising in practice. In short, we look for deeds not words."
— J. Hammersley [176]

The course title "Concrete Mathematics" was originally intended as an antidote to "Abstract Mathematics," since concrete classical results were rapidly being swept out of the modern mathematical curriculum by a new wave of abstract ideas popularly called the "New Math." Abstract mathematics is a wonderful subject, and there's nothing wrong with it: It's beautiful, general, and useful. But its adherents had become deluded that the rest of mathematics was inferior and no longer worthy of attention. The goal of generalization had become so fashionable that a generation of mathematicians had become unable to relish beauty in the particular, to enjoy the challenge of solving quantitative problems, or to appreciate the value of technique. Abstract mathematics was becoming inbred and losing touch with reality; mathematical education needed a concrete counterweight in order to restore a healthy balance.

When DEK taught Concrete Mathematics at Stanford for the first time, he explained the somewhat strange title by saying that it was his attempt to teach a math course that was hard instead of soft. He announced that, contrary to the expectations of some of his colleagues, he was *not* going to teach the Theory of Aggregates, nor Stone's Embedding Theorem, nor even the Stone–Čech compactification. (Several students from the civil engineering department got up and quietly left the room.)

"The heart of mathematics consists of concrete examples and concrete problems."
—P. R. Halmos [172]

Although Concrete Mathematics began as a reaction against other trends, the main reasons for its existence were positive instead of negative. And as the course continued its popular place in the curriculum, its subject matter "solidified" and proved to be valuable in a variety of new applications. Meanwhile, independent confirmation for the appropriateness of the name came from another direction, when Z. A. Melzak published two volumes entitled *Companion to Concrete Mathematics* [267].

"It is downright sinful to teach the abstract before the concrete."
—Z. A. Melzak [267]

The material of concrete mathematics may seem at first to be a disparate bag of tricks, but practice makes it into a disciplined set of tools. Indeed, the techniques have an underlying unity and a strong appeal for many people. When another one of the authors (RLG) first taught the course in 1979, the students had such fun that they decided to hold a class reunion a year later.

But what exactly is Concrete Mathematics? It is a blend of CONtinuous and disCRETE mathematics. More concretely, it is the controlled manipulation of mathematical formulas, using a collection of techniques for solving problems. Once you, the reader, have learned the material in this book, all you will need is a cool head, a large sheet of paper, and fairly decent handwriting in order to evaluate horrendous-looking sums, to solve complex recurrence relations, and to discover subtle patterns in data. You will be so fluent in algebraic techniques that you will often find it easier to obtain exact results than to settle for approximate answers that are valid only in a limiting sense.

Concrete Mathematics is a bridge to abstract mathematics.

The major topics treated in this book include sums, recurrences, elementary number theory, binomial coefficients, generating functions, discrete probability, and asymptotic methods. The emphasis is on manipulative technique rather than on existence theorems or combinatorial reasoning; the goal is for each reader to become as familiar with discrete operations (like the greatest-integer function and finite summation) as a student of calculus is familiar with continuous operations (like the absolute-value function and indefinite integration).

"The advanced reader who skips parts that appear too elementary may miss more than the less advanced reader who skips parts that appear too complex."
—G. Pólya [297]

Notice that this list of topics is quite different from what is usually taught nowadays in undergraduate courses entitled "Discrete Mathematics." Therefore the subject needs a distinctive name, and "Concrete Mathematics" has proved to be as suitable as any other.

(We're not bold enough to try Distinuous Mathematics.)

The original textbook for Stanford's course on concrete mathematics was the "Mathematical Preliminaries" section in *The Art of Computer Programming* [207]. But the presentation in those 110 pages is quite terse, so another author (OP) was inspired to draft a lengthy set of supplementary notes. The present book is an outgrowth of those notes; it is an expansion of, and a more leisurely introduction to, the material of Mathematical Preliminaries. Some of the more advanced parts have been omitted; on the other hand, several topics not found there have been included here so that the story will be complete.

"... a concrete life preserver thrown to students sinking in a sea of abstraction."
— W. Gottschalk

The authors have enjoyed putting this book together because the subject began to jell and to take on a life of its own before our eyes; this book almost seemed to write itself. Moreover, the somewhat unconventional approaches we have adopted in several places have seemed to fit together so well, after these years of experience, that we can't help feeling that this book is a kind of manifesto about our favorite way to do mathematics. So we think the book has turned out to be a tale of mathematical beauty and surprise, and we hope that our readers will share at least ϵ of the pleasure we had while writing it.

Since this book was born in a university setting, we have tried to capture the spirit of a contemporary classroom by adopting an informal style. Some people think that mathematics is a serious business that must always be cold and dry; but we think mathematics is fun, and we aren't ashamed to admit the fact. Why should a strict boundary line be drawn between work and play? Concrete mathematics is full of appealing patterns; the manipulations are not always easy, but the answers can be astonishingly attractive. The joys and sorrows of mathematical work are reflected explicitly in this book because they are part of our lives.

Math graffiti:

Kilroy wasn't Haar.
Free the group.
Nuke the kernel.
Power to the n.
$N{=}1 \Rightarrow P{=}NP$.

Students always know better than their teachers, so we have asked the first students of this material to contribute their frank opinions, as "graffiti" in the margins. Some of these marginal markings are merely corny, some are profound; some of them warn about ambiguities or obscurities, others are typical comments made by wise guys in the back row; some are positive, some are negative, some are zero. But they all are real indications of feelings that should make the text material easier to assimilate. (The inspiration for such marginal notes comes from a student handbook entitled *Approaching Stanford*, where the official university line is counterbalanced by the remarks of outgoing students. For example, Stanford says, "There are a few things you cannot miss in this amorphous shape which is Stanford"; the margin says, "Amorphous ... what the h*** does that mean? Typical of the pseudo-intellectualism around here." Stanford: "There is no end to the potential of a group of students living together." Graffito: "Stanford dorms are like zoos without a keeper.")

I have only a marginal interest in this subject.

This was the most enjoyable course I've ever had. But it might be nice to summarize the material as you go along.

The margins also include direct quotations from famous mathematicians of past generations, giving the actual words in which they announced some of their fundamental discoveries. Somehow it seems appropriate to mix the words of Leibniz, Euler, Gauss, and others with those of the people who will be continuing the work. Mathematics is an ongoing endeavor for people everywhere; many strands are being woven into one rich fabric.

This book contains more than 500 exercises, divided into six categories:

I see: Concrete mathematics means drilling.

- ***Warmups*** are exercises that EVERY READER should try to do when first reading the material.
- ***Basics*** are exercises to develop facts that are best learned by trying one's own derivation rather than by reading somebody else's.
- ***Homework exercises*** are problems intended to deepen an understanding of material in the current chapter.
- ***Exam problems*** typically involve ideas from two or more chapters simultaneously; they are generally intended for use in take-home exams (not for in-class exams under time pressure).
- ***Bonus problems*** go beyond what an average student of concrete mathematics is expected to handle while taking a course based on this book; they extend the text in interesting ways.
- ***Research problems*** may or may not be humanly solvable, but the ones presented here seem to be worth a try (without time pressure).

The homework was tough but I learned a lot. It was worth every hour.

Take-home exams are vital — keep them.

Exams were harder than the homework led me to expect.

Answers to all the exercises appear in Appendix A, often with additional information about related results. (Of course, the "answers" to research problems are incomplete; but even in these cases, partial results or hints are given that might prove to be helpful.) Readers are encouraged to look at the answers, especially the answers to the warmup problems, but only AFTER making a serious attempt to solve the problem without peeking.

Cheaters may pass this course by just copying the answers, but they're only cheating themselves.

We have tried in Appendix C to give proper credit to the sources of each exercise, since a great deal of creativity and/or luck often goes into the design of an instructive problem. Mathematicians have unfortunately developed a tradition of borrowing exercises without any acknowledgment; we believe that the opposite tradition, practiced for example by books and magazines about chess (where names, dates, and locations of original chess problems are routinely specified) is far superior. However, we have not been able to pin down the sources of many problems that have become part of the folklore. If any reader knows the origin of an exercise for which our citation is missing or inaccurate, we would be glad to learn the details so that we can correct the omission in subsequent editions of this book.

Difficult exams don't take into account students who have other classes to prepare for.

The typeface used for mathematics throughout this book is a new design by Hermann Zapf [227], commissioned by the American Mathematical Society and developed with the help of a committee that included B. Beeton, R. P. Boas, L. K. Durst, D. E. Knuth, P. Murdock, R. S. Palais, P. Renz, E. Swanson, S. B. Whidden, and W. B. Woolf. The underlying philosophy of Zapf's design is to capture the flavor of mathematics as it might be written by a mathematician with excellent handwriting. A handwritten rather than mechanical style is appropriate because people generally create mathematics with pen, pencil, *I'm unaccustomed to this face.*

or chalk. (For example, one of the trademarks of the new design is the symbol for zero, '0', which is slightly pointed at the top because a handwritten zero rarely closes together smoothly when the curve returns to its starting point.) The letters are upright, not italic, so that subscripts, superscripts, and accents are more easily fitted with ordinary symbols. This new type family has been named *AMS Euler*, after the great Swiss mathematician Leonhard Euler (1707–1783) who discovered so much of mathematics as we know it today. The alphabets include Euler Text ($\mathrm{A}\mathrm{a}\,\mathrm{B}\mathrm{b}\,\mathrm{C}\mathrm{c}$ through $\mathrm{X}\mathrm{x}\,\mathrm{Y}\mathrm{y}\,\mathrm{Z}\mathrm{z}$), Euler Fraktur ($\mathfrak{A}\mathfrak{a}\,\mathfrak{B}\mathfrak{b}\,\mathfrak{C}\mathfrak{c}$ through $\mathfrak{X}\mathfrak{x}\,\mathfrak{Y}\mathfrak{y}\,\mathfrak{Z}\mathfrak{z}$), and Euler Script Capitals ($\mathcal{A}\,\mathcal{B}\,\mathcal{C}$ through $\mathcal{X}\,\mathcal{Y}\,\mathcal{Z}$), as well as Euler Greek ($\mathrm{A}\alpha\,\mathrm{B}\beta\,\Gamma\gamma$ through $\mathrm{X}\chi\,\Psi\psi\,\Omega\omega$) and special symbols such as $\wp$ and $\aleph$. We are especially pleased to be able to inaugurate the Euler family of typefaces in this book, because Leonhard Euler's spirit truly lives on every page: Concrete mathematics is Eulerian mathematics.

Dear prof: Thanks for (1) the puns, (2) the subject matter.

The authors are extremely grateful to Andrei Broder, Ernst Mayr, Andrew Yao, and Frances Yao, who contributed greatly to this book during the years that they taught Concrete Mathematics at Stanford. Furthermore we offer 1024 thanks to the teaching assistants who creatively transcribed what took place in class each year and who helped to design the examination questions; their names are listed in Appendix C. This book, which is essentially a compendium of sixteen years' worth of lecture notes, would have been impossible without their first-rate work.

I don't see how what I've learned will ever help me.

Many other people have helped to make this book a reality. For example, we wish to commend the students at Brown, Columbia, CUNY, Princeton, Rice, and Stanford who contributed the choice graffiti and helped to debug our first drafts. Our contacts at Addison-Wesley were especially efficient and helpful; in particular, we wish to thank our publisher (Peter Gordon), production supervisor (Bette Aaronson), designer (Roy Brown), and copy editor (Lyn Dupré). The National Science Foundation and the Office of Naval Research have given invaluable support. Cheryl Graham was tremendously helpful as we prepared the index. And above all, we wish to thank our wives (Fan, Jill, and Amy) for their patience, support, encouragement, and ideas.

I had a lot of trouble in this class, but I know it sharpened my math skills and my thinking skills.

This second edition features a new Section 5.8, which describes some important ideas that Doron Zeilberger discovered shortly after the first edition went to press. Additional improvements to the first printing can also be found on almost every page.

We have tried to produce a perfect book, but we are imperfect authors. Therefore we solicit help in correcting any mistakes that we've made. A reward of \$2.56 will gratefully be conveyed to anyone who is the first to report any error, whether it is mathematical, historical, or typographical.

I would advise the casual student to stay away from this course.

Murray Hill, New Jersey — RLG
and Stanford, California DEK
May 1988 and October 1993 OP

A Note on Notation

SOME OF THE SYMBOLISM in this book has not (yet?) become standard. Here is a list of notations that might be unfamiliar to readers who have learned similar material from other books, together with the page numbers where these notations are explained. (See the general index, at the end of the book, for references to more standard notations.)

Notation	*Name*	*Page*
$\ln x$	natural logarithm: $\log_e x$	276
$\lg x$	binary logarithm: $\log_2 x$	70
$\log x$	common logarithm: $\log_{10} x$	449
$\lfloor x \rfloor$	floor: $\max\{\, n \mid n \leqslant x,\ \text{integer } n \,\}$	67
$\lceil x \rceil$	ceiling: $\min\{\, n \mid n \geqslant x,\ \text{integer } n \,\}$	67
$x \bmod y$	remainder: $x - y\lfloor x/y \rfloor$	82
$\{x\}$	fractional part: $x \bmod 1$	70
$\sum f(x)\,\delta x$	indefinite summation	48
$\sum_a^b f(x)\,\delta x$	definite summation	49
$x^{\underline{n}}$	falling factorial power: $x!/(x-n)!$	47, 211
$x^{\overline{n}}$	rising factorial power: $\Gamma(x+n)/\Gamma(x)$	48, 211
$n¡$	subfactorial: $n!/0! - n!/1! + \cdots + (-1)^n n!/n!$	194
$\Re z$	real part: x, if $z = x + iy$	64
$\Im z$	imaginary part: y, if $z = x + iy$	64
H_n	harmonic number: $1/1 + \cdots + 1/n$	29
$H_n^{(x)}$	generalized harmonic number: $1/1^x + \cdots + 1/n^x$	277

If you don't understand what the x denotes at the bottom of this page, try asking your Latin professor instead of your math professor.

$f^{(m)}(z)$	mth derivative of f at z	470
$\left[{n \atop m}\right]$	Stirling cycle number (the "first kind")	259
$\left\{{n \atop m}\right\}$	Stirling subset number (the "second kind")	258
$\left\langle{n \atop m}\right\rangle$	Eulerian number	267
$\left\langle\!\!\left\langle{n \atop m}\right\rangle\!\!\right\rangle$	Second-order Eulerian number	270
$(a_m \ldots a_0)_b$	radix notation for $\sum_{k=0}^{m} a_k b^k$	11
$K(a_1, \ldots, a_n)$	continuant polynomial	302
$F\left({a, b \atop c} \middle\vert z\right)$	hypergeometric function	205
$\#A$	cardinality: number of elements in the set A	39
$[z^n]\, f(z)$	coefficient of z^n in $f(z)$	197
$[\alpha \mathinner{..} \beta]$	closed interval: the set $\{x \mid \alpha \leqslant x \leqslant \beta\}$	73
$[m = n]$	1 if $m = n$, otherwise 0*	24
$[m \backslash n]$	1 if m divides n, otherwise 0*	102
$[m \backslash\backslash n]$	1 if m exactly divides n, otherwise 0*	146
$[m \perp n]$	1 if m is relatively prime to n, otherwise 0*	115

Prestressed concrete mathematics is concrete mathematics that's preceded by a bewildering list of notations.

*In general, if S is any statement that can be true or false, the bracketed notation $[S]$ stands for 1 if S is true, 0 otherwise.

Throughout this text, we use single-quote marks ('. . . ') to delimit text as it is *written*, double-quote marks (". . . ") for a phrase as it is *spoken*. Thus, the string of letters 'string' is sometimes called a "string."

Also 'nonstring' is a string.

An expression of the form 'a/bc' means the same as '$a/(bc)$'. Moreover, $\log x/\log y = (\log x)/(\log y)$ and $2n! = 2(n!)$.

Contents

This page intentionally left blank

3

Integer Functions

WHOLE NUMBERS constitute the backbone of discrete mathematics, and we often need to convert from fractions or arbitrary real numbers to integers. Our goal in this chapter is to gain familiarity and fluency with such conversions and to learn some of their remarkable properties.

3.1 FLOORS AND CEILINGS

We start by covering the floor (greatest integer) and ceiling (least integer) functions, which are defined for all real x as follows:

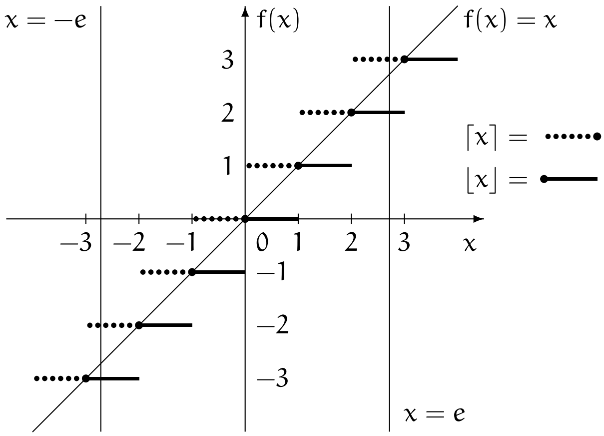
$$\begin{aligned} \lfloor x \rfloor &= \text{the greatest integer less than or equal to } x\,; \\ \lceil x \rceil &= \text{the least integer greater than or equal to } x\,. \end{aligned} \qquad (3.1)$$

Kenneth E. Iverson introduced this notation, as well as the names "floor" and "ceiling," early in the 1960s [191, page 12]. He found that typesetters could handle the symbols by shaving the tops and bottoms off of '[' and ']'. His notation has become sufficiently popular that floor and ceiling brackets can now be used in a technical paper without an explanation of what they mean. Until recently, people had most often been writing '[x]' for the greatest integer $\leqslant x$, without a good equivalent for the least integer function. Some authors had even tried to use ']x['—with a predictable lack of success.

)Ouch.(

Besides variations in notation, there are variations in the functions themselves. For example, some pocket calculators have an INT function, defined as $\lfloor x \rfloor$ when x is positive and $\lceil x \rceil$ when x is negative. The designers of these calculators probably wanted their INT function to satisfy the identity $\mathrm{INT}(-x) = -\mathrm{INT}(x)$. But we'll stick to our floor and ceiling functions, because they have even nicer properties than this.

One good way to become familiar with the floor and ceiling functions is to understand their graphs, which form staircase-like patterns above and below the line $f(x) = x$:



We see from the graph that, for example,

$$\lfloor e \rfloor = 2\,, \qquad \lfloor -e \rfloor = -3\,,$$
$$\lceil e \rceil = 3\,, \qquad \lceil -e \rceil = -2\,,$$

since $e = 2.71828\ldots$.

By staring at this illustration we can observe several facts about floors and ceilings. First, since the floor function lies on or below the diagonal line $f(x) = x$, we have $\lfloor x \rfloor \leqslant x$; similarly $\lceil x \rceil \geqslant x$. (This, of course, is quite obvious from the definition.) The two functions are equal precisely at the integer points:

$$\lfloor x \rfloor = x \quad\iff\quad x \text{ is an integer} \quad\iff\quad \lceil x \rceil = x\,.$$

(We use the notation '$\iff$' to mean "if and only if.") Furthermore, when they differ the ceiling is exactly 1 higher than the floor:

$$\lceil x \rceil - \lfloor x \rfloor = [x \text{ is not an integer}]\,. \tag{3.2}$$

Cute.
By Iverson's bracket convention, this is a complete equation.

If we shift the diagonal line down one unit, it lies completely below the floor function, so $x - 1 < \lfloor x \rfloor$; similarly $x + 1 > \lceil x \rceil$. Combining these observations gives us

$$x - 1 < \lfloor x \rfloor \leqslant x \leqslant \lceil x \rceil < x + 1\,. \tag{3.3}$$

Finally, the functions are reflections of each other about both axes:

$$\lfloor -x \rfloor = -\lceil x \rceil\,; \qquad \lceil -x \rceil = -\lfloor x \rfloor\,. \tag{3.4}$$

Thus each is easily expressible in terms of the other. This fact helps to explain why the ceiling function once had no notation of its own. But we see ceilings often enough to warrant giving them special symbols, just as we have adopted special notations for rising powers as well as falling powers. Mathematicians have long had both sine and cosine, tangent and cotangent, secant and cosecant, max and min; now we also have both floor and ceiling.

Next week we're getting walls.

To actually prove properties about the floor and ceiling functions, rather than just to observe such facts graphically, the following four rules are especially useful:

$$\begin{aligned} \lfloor x \rfloor = n \quad &\iff \quad n \leqslant x < n+1, && \text{(a)} \\ \lfloor x \rfloor = n \quad &\iff \quad x-1 < n \leqslant x, && \text{(b)} \\ \lceil x \rceil = n \quad &\iff \quad n-1 < x \leqslant n, && \text{(c)} \\ \lceil x \rceil = n \quad &\iff \quad x \leqslant n < x+1. && \text{(d)} \end{aligned} \tag{3.5}$$

(We assume in all four cases that n is an integer and that x is real.) Rules (a) and (c) are immediate consequences of definition (3.1); rules (b) and (d) are the same but with the inequalities rearranged so that n is in the middle.

It's possible to move an integer term in or out of a floor (or ceiling):

$$\lfloor x+n \rfloor \;=\; \lfloor x \rfloor + n, \qquad \text{integer } n. \tag{3.6}$$

(Because rule (3.5(a)) says that this assertion is equivalent to the inequalities $\lfloor x \rfloor + n \leqslant x+n < \lfloor x \rfloor + n + 1$.) But similar operations, like moving out a constant factor, cannot be done in general. For example, we have $\lfloor nx \rfloor \neq n\lfloor x \rfloor$ when $n = 2$ and $x = 1/2$. This means that floor and ceiling brackets are comparatively inflexible. We are usually happy if we can get rid of them or if we can prove anything at all when they are present.

It turns out that there are many situations in which floor and ceiling brackets are redundant, so that we can insert or delete them at will. For example, any inequality between a real and an integer is equivalent to a floor or ceiling inequality between integers:

$$\begin{aligned} x < n \quad &\iff \quad \lfloor x \rfloor < n, && \text{(a)} \\ n < x \quad &\iff \quad n < \lceil x \rceil, && \text{(b)} \\ x \leqslant n \quad &\iff \quad \lceil x \rceil \leqslant n, && \text{(c)} \\ n \leqslant x \quad &\iff \quad n \leqslant \lfloor x \rfloor. && \text{(d)} \end{aligned} \tag{3.7}$$

These rules are easily proved. For example, if $x < n$ then surely $\lfloor x \rfloor < n$, since $\lfloor x \rfloor \leqslant x$. Conversely, if $\lfloor x \rfloor < n$ then we must have $x < n$, since $x < \lfloor x \rfloor + 1$ and $\lfloor x \rfloor + 1 \leqslant n$.

It would be nice if the four rules in (3.7) were as easy to remember as they are to prove. Each inequality without floor or ceiling corresponds to the same inequality with floor or with ceiling; but we need to think twice before deciding which of the two is appropriate.

The difference between x and $\lfloor x \rfloor$ is called the *fractional part* of x, and it arises often enough in applications to deserve its own notation:

$$\{x\} \;=\; x - \lfloor x \rfloor\,. \qquad (3.8)$$

Hmmm. We'd better not write $\{x\}$ for the fractional part when it could be confused with the set containing x as its only element.

We sometimes call $\lfloor x \rfloor$ the *integer part* of x, since $x = \lfloor x \rfloor + \{x\}$. If a real number x can be written in the form $x = n + \theta$, where n is an integer and $0 \leqslant \theta < 1$, we can conclude by (3.5(a)) that $n = \lfloor x \rfloor$ and $\theta = \{x\}$.

Identity (3.6) doesn't hold if n is an arbitrary real. But we can deduce that there are only two possibilities for $\lfloor x + y \rfloor$ in general: If we write $x = \lfloor x \rfloor + \{x\}$ and $y = \lfloor y \rfloor + \{y\}$, then we have $\lfloor x + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor + \lfloor \{x\} + \{y\} \rfloor$. And since $0 \leqslant \{x\} + \{y\} < 2$, we find that sometimes $\lfloor x + y \rfloor$ is $\lfloor x \rfloor + \lfloor y \rfloor$, otherwise it's $\lfloor x \rfloor + \lfloor y \rfloor + 1$.

The second case occurs if and only if there's a "carry" at the position of the decimal point, when the fractional parts $\{x\}$ and $\{y\}$ are added together.

3.2 FLOOR/CEILING APPLICATIONS

We've now seen the basic tools for handling floors and ceilings. Let's put them to use, starting with an easy problem: What's $\lceil \lg 35 \rceil$? (Following a convention that many authors have proposed independently, we use 'lg' to denote the base-2 logarithm.) Well, since $2^5 < 35 \leqslant 2^6$, we can take logs to get $5 < \lg 35 \leqslant 6$; so relation (3.5(c)) tells us that $\lceil \lg 35 \rceil = 6$.

Note that the number 35 is six bits long when written in radix 2 notation: $35 = (100011)_2$. Is it always true that $\lceil \lg n \rceil$ is the length of n written in binary? Not quite. We also need six bits to write $32 = (100000)_2$. So $\lceil \lg n \rceil$ is the wrong answer to the problem. (It fails only when n is a power of 2, but that's infinitely many failures.) We can find a correct answer by realizing that it takes m bits to write each number n such that $2^{m-1} \leqslant n < 2^m$; thus (3.5(a)) tells us that $m - 1 = \lfloor \lg n \rfloor$, so $m = \lfloor \lg n \rfloor + 1$. That is, we need $\lfloor \lg n \rfloor + 1$ bits to express n in binary, for all $n > 0$. Alternatively, a similar derivation yields the answer $\lceil \lg(n+1) \rceil$; this formula holds for $n = 0$ as well, if we're willing to say that it takes zero bits to write $n = 0$ in binary.

Let's look next at expressions with several floors or ceilings. What is $\lceil \lfloor x \rfloor \rceil$? Easy — since $\lfloor x \rfloor$ is an integer, $\lceil \lfloor x \rfloor \rceil$ is just $\lfloor x \rfloor$. So is any other expression with an innermost $\lfloor x \rfloor$ surrounded by any number of floors or ceilings.

Here's a tougher problem: Prove or disprove the assertion

$$\bigl\lfloor \sqrt{\lfloor x \rfloor} \bigr\rfloor \;=\; \lfloor \sqrt{x} \rfloor\,, \qquad \text{real } x \geqslant 0. \qquad (3.9)$$

Equality obviously holds when x is an integer, because $x = \lfloor x \rfloor$. And there's equality in the special cases $\pi = 3.14159\ldots$, $e = 2.71828\ldots$, and $\phi = (1 + \sqrt{5})/2 = 1.61803\ldots$, because we get $1 = 1$. Our failure to find a counterexample suggests that equality holds in general, so let's try to prove it.

(Of course π, e, and ϕ are the obvious first real numbers to try, aren't they?)

Skepticism is healthy only to a limited extent. Being skeptical about proofs and programs (particularly your own) will probably keep your grades healthy and your job fairly secure. But applying that much skepticism will probably also keep you shut away working all the time, instead of letting you get out for exercise and relaxation. Too much skepticism is an open invitation to the state of rigor mortis, where you become so worried about being correct and rigorous that you never get anything finished.
—A skeptic

Incidentally, when we're faced with a "prove or disprove," we're usually better off trying first to disprove with a counterexample, for two reasons: A disproof is potentially easier (we need just one counterexample); and nit-picking arouses our creative juices. Even if the given assertion is true, our search for a counterexample often leads us to a proof, as soon as we see why a counterexample is impossible. Besides, it's healthy to be skeptical.

If we try to prove that $\lfloor\sqrt{\lfloor x\rfloor}\rfloor = \lfloor\sqrt{x}\rfloor$ with the help of calculus, we might start by decomposing x into its integer and fractional parts $\lfloor x\rfloor + \{x\} = n + \theta$ and then expanding the square root using the binomial theorem: $(n+\theta)^{1/2} = n^{1/2} + n^{-1/2}\theta/2 - n^{-3/2}\theta^2/8 + \cdots$. But this approach gets pretty messy.

It's much easier to use the tools we've developed. Here's a possible strategy: Somehow strip off the outer floor and square root of $\lfloor\sqrt{\lfloor x\rfloor}\rfloor$, then remove the inner floor, then add back the outer stuff to get $\lfloor\sqrt{x}\rfloor$. OK. We let $m = \lfloor\sqrt{\lfloor x\rfloor}\rfloor$ and invoke (3.5(a)), giving $m \leqslant \sqrt{\lfloor x\rfloor} < m+1$. That removes the outer floor bracket without losing any information. Squaring, since all three expressions are nonnegative, we have $m^2 \leqslant \lfloor x\rfloor < (m+1)^2$. That gets rid of the square root. Next we remove the floor, using (3.7(d)) for the left inequality and (3.7(a)) for the right: $m^2 \leqslant x < (m+1)^2$. It's now a simple matter to retrace our steps, taking square roots to get $m \leqslant \sqrt{x} < m+1$ and invoking (3.5(a)) to get $m = \lfloor\sqrt{x}\rfloor$. Thus $\lfloor\sqrt{\lfloor x\rfloor}\rfloor = m = \lfloor\sqrt{x}\rfloor$; the assertion is true. Similarly, we can prove that

$$\lceil\sqrt{\lceil x\rceil}\rceil = \lceil\sqrt{x}\,\rceil, \qquad \text{real } x \geqslant 0.$$

The proof we just found doesn't rely heavily on the properties of square roots. A closer look shows that we can generalize the ideas and prove much more: Let $f(x)$ be any continuous, monotonically increasing function on an interval of the real numbers, with the property that

$$f(x) = \text{integer} \quad\Longrightarrow\quad x = \text{integer}.$$

(The symbol '$\Longrightarrow$' means "implies.") Then we have

(This observation was made by R. J. McEliece when he was an undergrad.)

$$\lfloor f(x)\rfloor = \lfloor f(\lfloor x\rfloor)\rfloor \quad\text{and}\quad \lceil f(x)\rceil = \lceil f(\lceil x\rceil)\rceil, \tag{3.10}$$

whenever $f(x)$, $f(\lfloor x\rfloor)$, and $f(\lceil x\rceil)$ are defined. Let's prove this general property for ceilings, since we did floors earlier and since the proof for floors is almost the same. If $x = \lceil x\rceil$, there's nothing to prove. Otherwise $x < \lceil x\rceil$, and $f(x) < f(\lceil x\rceil)$ since f is increasing. Hence $\lceil f(x)\rceil \leqslant \lceil f(\lceil x\rceil)\rceil$, since $\lceil\,\rceil$ is nondecreasing. If $\lceil f(x)\rceil < \lceil f(\lceil x\rceil)\rceil$, there must be a number y such that $x \leqslant y < \lceil x\rceil$ and $f(y) = \lceil f(x)\rceil$, since f is continuous. This y is an integer, because of f's special property. But there cannot be an integer strictly between $\lfloor x\rfloor$ and $\lceil x\rceil$. This contradiction implies that we must have $\lceil f(x)\rceil = \lceil f(\lceil x\rceil)\rceil$.

An important special case of this theorem is worth noting explicitly:

$$\left\lfloor \frac{x+m}{n} \right\rfloor = \left\lfloor \frac{\lfloor x \rfloor + m}{n} \right\rfloor \qquad \text{and} \qquad \left\lceil \frac{x+m}{n} \right\rceil = \left\lceil \frac{\lceil x \rceil + m}{n} \right\rceil, \quad (3.11)$$

if m and n are integers and the denominator n is positive. For example, let $m = 0$; we have $\lfloor \lfloor \lfloor x/10 \rfloor/10 \rfloor/10 \rfloor = \lfloor x/1000 \rfloor$. Dividing thrice by 10 and throwing off digits is the same as dividing by 1000 and tossing the remainder.

Let's try now to prove or disprove another statement:

$$\left\lceil \sqrt{\lfloor x \rfloor} \right\rceil \stackrel{?}{=} \lceil \sqrt{x} \rceil, \qquad \text{real } x \geqslant 0.$$

This works when $x = \pi$ and $x = e$, but it fails when $x = \phi$; so we know that it isn't true in general.

Before going any further, let's digress a minute to discuss different levels of problems that might appear in books about mathematics:

Level 1. Given an explicit object x and an explicit property $P(x)$, *prove* that $P(x)$ is true. For example, "Prove that $\lfloor \pi \rfloor = 3$." Here the problem involves finding a proof of some purported fact.

Level 2. Given an explicit set X and an explicit property $P(x)$, prove that $P(x)$ is true *for all* $x \in X$. For example, "Prove that $\lfloor x \rfloor \leqslant x$ for all real x." Again the problem involves finding a proof, but the proof this time must be general. We're doing algebra, not just arithmetic.

Level 3. Given an explicit set X and an explicit property $P(x)$, prove *or disprove* that $P(x)$ is true for all $x \in X$. For example, "Prove or disprove that $\left\lceil \sqrt{\lfloor x \rfloor} \right\rceil = \lceil \sqrt{x} \rceil$ for all real $x \geqslant 0$." Here there's an additional level of uncertainty; the outcome might go either way. This is closer to the real situation a mathematician constantly faces: Assertions that get into books tend to be true, but new things have to be looked at with a jaundiced eye. If the statement is false, our job is to find a counterexample. If the statement is true, we must find a proof as in level 2.

In my other texts "prove or disprove" seems to mean the same as "prove," about 99.44% of the time; but not in this book.

Level 4. Given an explicit set X and an explicit property $P(x)$, find a *necessary and sufficient condition* $Q(x)$ that $P(x)$ is true. For example, "Find a necessary and sufficient condition that $\lfloor x \rfloor \geqslant \lceil x \rceil$." The problem is to find Q such that $P(x) \iff Q(x)$. Of course, there's always a trivial answer; we can take $Q(x) = P(x)$. But the implied requirement is to find a condition that's as simple as possible. Creativity is required to discover a simple condition that will work. (For example, in this case, "$\lfloor x \rfloor \geqslant \lceil x \rceil \iff x$ is an integer.") The extra element of discovery needed to find $Q(x)$ makes this sort of problem more difficult, but it's more typical of what mathematicians must do in the "real world." Finally, of course, a proof must be given that $P(x)$ is true if and only if $Q(x)$ is true.

But no simpler.
—A. Einstein

Level 5. Given an explicit set X, find *an interesting property* P(x) of its elements. Now we're in the scary domain of pure research, where students might think that total chaos reigns. This is real mathematics. Authors of textbooks rarely dare to pose level 5 problems.

End of digression. But let's convert the last question we looked at from level 3 to level 4: What is a necessary and sufficient condition that $\lceil\sqrt{\lfloor x\rfloor}\,\rceil = \lceil\sqrt{x}\,\rceil$? We have observed that equality holds when $x = 3.142$ but not when $x = 1.618$; further experimentation shows that it fails also when x is between 9 and 10. Oho. Yes. We see that bad cases occur whenever $m^2 < x < m^2+1$, since this gives m on the left and $m+1$ on the right. In all other cases where $\sqrt{x}$ is defined, namely when $x = 0$ or $m^2 + 1 \leqslant x \leqslant (m+1)^2$, we get equality. The following statement is therefore necessary and sufficient for equality: Either x is an integer or $\sqrt{\lfloor x\rfloor}$ isn't.

Home of the Toledo Mudhens.

For our next problem let's consider a handy new notation, suggested by C. A. R. Hoare and Lyle Ramshaw, for intervals of the real line: $[\alpha\mathinner{..}\beta]$ denotes the set of real numbers x such that $\alpha \leqslant x \leqslant \beta$. This set is called a *closed interval* because it contains both endpoints α and β. The interval containing neither endpoint, denoted by $(\alpha\mathinner{..}\beta)$, consists of all x such that $\alpha < x < \beta$; this is called an *open interval*. And the intervals $[\alpha\mathinner{..}\beta)$ and $(\alpha\mathinner{..}\beta]$, which contain just one endpoint, are defined similarly and called *half-open*.

(Or, by pessimists, half-closed.)

How many integers are contained in such intervals? The half-open intervals are easier, so we start with them. In fact half-open intervals are almost always nicer than open or closed intervals. For example, they're additive — we can combine the half-open intervals $[\alpha\mathinner{..}\beta)$ and $[\beta\mathinner{..}\gamma)$ to form the half-open interval $[\alpha\mathinner{..}\gamma)$. This wouldn't work with open intervals because the point β would be excluded, and it could cause problems with closed intervals because β would be included twice.

Back to our problem. The answer is easy if α and β are integers: Then $[\alpha\mathinner{..}\beta)$ contains the $\beta-\alpha$ integers $\alpha, \alpha+1, \ldots, \beta-1$, assuming that $\alpha \leqslant \beta$. Similarly $(\alpha\mathinner{..}\beta]$ contains $\beta - \alpha$ integers in such a case. But our problem is harder, because α and β are arbitrary reals. We can convert it to the easier problem, though, since

$$\begin{aligned} \alpha \leqslant n < \beta \quad &\iff \quad \lceil\alpha\rceil \leqslant n < \lceil\beta\rceil\,, \\ \alpha < n \leqslant \beta \quad &\iff \quad \lfloor\alpha\rfloor < n \leqslant \lfloor\beta\rfloor\,, \end{aligned}$$

when n is an integer, according to (3.7). The intervals on the right have integer endpoints and contain the same number of integers as those on the left, which have real endpoints. So the interval $[\alpha\mathinner{..}\beta)$ contains exactly $\lceil\beta\rceil - \lceil\alpha\rceil$ integers, and $(\alpha\mathinner{..}\beta]$ contains $\lfloor\beta\rfloor - \lfloor\alpha\rfloor$. This is a case where we actually want to introduce floor or ceiling brackets, instead of getting rid of them.

By the way, there's a mnemonic for remembering which case uses floors and which uses ceilings: Half-open intervals that include the left endpoint but not the right (such as $0 \leqslant \theta < 1$) are slightly more common than those that include the right endpoint but not the left; and floors are slightly more common than ceilings. So by Murphy's Law, the correct rule is the opposite of what we'd expect — ceilings for $[\alpha\,..\,\beta)$ and floors for $(\alpha\,..\,\beta]$.

Just like we can remember the date of Columbus's departure by singing, "In fourteen hundred and ninety-three/ Columbus sailed the deep blue sea."

Similar analyses show that the closed interval $[\alpha\,..\,\beta]$ contains exactly $\lfloor\beta\rfloor - \lceil\alpha\rceil + 1$ integers and that the open interval $(\alpha\,..\,\beta)$ contains $\lceil\beta\rceil - \lfloor\alpha\rfloor - 1$; but we place the additional restriction $\alpha \neq \beta$ on the latter so that the formula won't ever embarrass us by claiming that an empty interval $(\alpha\,..\,\alpha)$ contains a total of -1 integers. To summarize, we've deduced the following facts:

interval	integers contained	restrictions
$[\alpha\,..\,\beta]$	$\lfloor\beta\rfloor - \lceil\alpha\rceil + 1$	$\alpha \leqslant \beta$,
$[\alpha\,..\,\beta)$	$\lceil\beta\rceil - \lceil\alpha\rceil$	$\alpha \leqslant \beta$,
$(\alpha\,..\,\beta]$	$\lfloor\beta\rfloor - \lfloor\alpha\rfloor$	$\alpha \leqslant \beta$,
$(\alpha\,..\,\beta)$	$\lceil\beta\rceil - \lfloor\alpha\rfloor - 1$	$\alpha < \beta$.

(3.12)

Now here's a problem we can't refuse. The Concrete Math Club has a casino (open only to purchasers of this book) in which there's a roulette wheel with one thousand slots, numbered 1 to 1000. If the number n that comes up on a spin is divisible by the floor of its cube root, that is, if

$$\lfloor\sqrt[3]{n}\rfloor \;\backslash\; n\,,$$

then it's a winner and the house pays us \$5; otherwise it's a loser and we must pay \$1. (The notation $a\backslash b$, read "a divides b," means that b is an exact multiple of a; Chapter 4 investigates this relation carefully.) Can we expect to make money if we play this game?

(A poll of the class at this point showed that 28 students thought it was a bad idea to play, 13 wanted to gamble, and the rest were too confused to answer.)

(So we hit them with the Concrete Math Club.)

We can compute the average winnings — that is, the amount we'll win (or lose) per play — by first counting the number W of winners and the number $L = 1000 - W$ of losers. If each number comes up once during 1000 plays, we win $5W$ dollars and lose L dollars, so the average winnings will be

$$\frac{5W - L}{1000} = \frac{5W - (1000 - W)}{1000} = \frac{6W - 1000}{1000}\,.$$

If there are 167 or more winners, we have the advantage; otherwise the advantage is with the house.

How can we count the number of winners among 1 through 1000? It's not hard to spot a pattern. The numbers from 1 through $2^3 - 1 = 7$ are all winners because $\lfloor\sqrt[3]{n}\rfloor = 1$ for each. Among the numbers $2^3 = 8$ through $3^3 - 1 = 26$, only the even numbers are winners. And among $3^3 = 27$ through $4^3 - 1 = 63$, only those divisible by 3 are. And so on.

The whole setup can be analyzed systematically if we use the summation techniques of Chapter 2, taking advantage of Iverson's convention about logical statements evaluating to 0 or 1:

$$\begin{aligned} W &= \sum_{n=1}^{1000} [n \text{ is a winner}] \\ &= \sum_{1\le n\le 1000} \bigl[\lfloor\sqrt[3]{n}\rfloor \backslash n\bigr] \;=\; \sum_{k,n} \bigl[k=\lfloor\sqrt[3]{n}\rfloor\bigr][k\backslash n][1\le n\le 1000] \\ &= \sum_{k,m,n} \bigl[k^3\le n<(k+1)^3\bigr][n=km][1\le n\le 1000] \\ &= 1+\sum_{k,m} \bigl[k^3\le km<(k+1)^3\bigr][1\le k<10] \\ &= 1+\sum_{k,m} \bigl[m\in\bigl[k^2\,..\,(k+1)^3/k\bigr)\bigr][1\le k<10] \\ &= 1+\sum_{1\le k<10} \bigl(\lceil k^2+3k+3+1/k\rceil-\lceil k^2\rceil\bigr) \\ &= 1+\sum_{1\le k<10} (3k+4) \;=\; 1+\frac{7+31}{2}\cdot 9 \;=\; 172\,. \end{aligned}$$

This derivation merits careful study. Notice that line 6 uses our formula (3.12) for the number of integers in a half-open interval. The only "difficult" maneuver is the decision made between lines 3 and 4 to treat $n = 1000$ as a special case. (The inequality $k^3 \le n < (k+1)^3$ does not combine easily with $1 \le n \le 1000$ when $k = 10$.) In general, boundary conditions tend to be the most critical part of $\sum$-manipulations.

True.

The bottom line says that $W = 172$; hence our formula for average winnings per play reduces to $(6\cdot 172 - 1000)/1000$ dollars, which is 3.2 cents. We can expect to be about \$3.20 richer after making 100 bets of \$1 each. (Of course, the house may have made some numbers more equal than others.)

Where did you say this casino is?

The casino problem we just solved is a dressed-up version of the more mundane question, "How many integers n, where $1 \le n \le 1000$, satisfy the relation $\lfloor\sqrt[3]{n}\rfloor \backslash n$?" Mathematically the two questions are the same. But sometimes it's a good idea to dress up a problem. We get to use more vocabulary (like "winners" and "losers"), which helps us to understand what's going on.

Let's get general. Suppose we change 1000 to 1000000, or to an even larger number, N. (We assume that the casino has connections and can get a bigger wheel.) Now how many winners are there?

The same argument applies, but we need to deal more carefully with the largest value of k, which we can call K for convenience:

$$K = \lfloor\sqrt[3]{N}\rfloor\,.$$

(Previously K was 10.) The total number of winners for general N comes to

$$\begin{aligned} W &= \sum_{1\leqslant k<K} (3k+4) + \sum_m \bigl[K^3 \leqslant Km \leqslant N\bigr] \\ &= \tfrac{1}{2}(7+3K+1)(K-1) + \sum_m \bigl[m \in [K^2 \mathinner{..} N/K]\bigr] \\ &= \tfrac{3}{2}K^2 + \tfrac{5}{2}K - 4 + \sum_m \bigl[m \in [K^2 \mathinner{..} N/K]\bigr] . \end{aligned}$$

We know that the remaining sum is $\lfloor N/K \rfloor - \lceil K^2 \rceil + 1 = \lfloor N/K \rfloor - K^2 + 1$; hence the formula

$$W = \lfloor N/K \rfloor + \tfrac{1}{2}K^2 + \tfrac{5}{2}K - 3 , \qquad K = \lfloor \sqrt[3]{N} \rfloor \tag{3.13}$$

gives the general answer for a wheel of size N.

The first two terms of this formula are approximately $N^{2/3} + \frac{1}{2}N^{2/3} = \frac{3}{2}N^{2/3}$, and the other terms are much smaller in comparison, when N is large. In Chapter 9 we'll learn how to derive expressions like

$$W = \tfrac{3}{2}N^{2/3} + O(N^{1/3}) ,$$

where $O(N^{1/3})$ stands for a quantity that is no more than a constant times $N^{1/3}$. Whatever the constant is, we know that it's independent of N; so for large N the contribution of the O-term to W will be quite small compared with $\frac{3}{2}N^{2/3}$. For example, the following table shows how close $\frac{3}{2}N^{2/3}$ is to W:

N	$\frac{3}{2}N^{2/3}$	W	% error
1,000	150.0	172	12.791
10,000	696.2	746	6.670
100,000	3231.7	3343	3.331
1,000,000	15000.0	15247	1.620
10,000,000	69623.8	70158	0.761
100,000,000	323165.2	324322	0.357
1,000,000,000	1500000.0	1502497	0.166

It's a pretty good approximation.

Approximate formulas are useful because they're simpler than formulas with floors and ceilings. However, the exact truth is often important, too, especially for the smaller values of N that tend to occur in practice. For example, the casino owner may have falsely assumed that there are only $\frac{3}{2}N^{2/3} = 150$ winners when $N = 1000$ (in which case there would be a 10¢ advantage for the house).

Our last application in this section looks at so-called spectra. We define the *spectrum* of a positive real number α to be an infinite multiset of integers,

$$\mathrm{Spec}(\alpha) \;=\; \{\lfloor\alpha\rfloor,\ \lfloor 2\alpha\rfloor,\ \lfloor 3\alpha\rfloor,\ \ldots\}.$$

(A multiset is like a set but it can have repeated elements.) For example, the spectrum of $1/2$ starts out $\{0,1,1,2,2,3,3,\ldots\}$.

... without lots of generality...

It's easy to prove that no two spectra are equal—that $\alpha \neq \beta$ implies $\mathrm{Spec}(\alpha) \neq \mathrm{Spec}(\beta)$. For, assuming without loss of generality that $\alpha < \beta$, there's a positive integer m such that $m(\beta-\alpha) \geqslant 1$. (In fact, any $m \geqslant \lceil 1/(\beta-\alpha)\rceil$ will do; but we needn't show off our knowledge of floors and ceilings all the time.) Hence $m\beta - m\alpha \geqslant 1$, and $\lfloor m\beta\rfloor > \lfloor m\alpha\rfloor$. Thus $\mathrm{Spec}(\beta)$ has fewer than m elements $\leqslant \lfloor m\alpha\rfloor$, while $\mathrm{Spec}(\alpha)$ has at least m.

"If x be an incommensurable number less than unity, one of the series of quantities m/x, $m/(1-x)$, where m is a whole number, can be found which shall lie between any given consecutive integers, and but one such quantity can be found."
—Rayleigh [304]

Spectra have many beautiful properties. For example, consider the two multisets

$$\begin{aligned}\mathrm{Spec}(\sqrt{2}\,) &= \{1,2,4,5,7,8,9,11,12,14,15,16,18,19,21,22,24,\ldots\},\\ \mathrm{Spec}(2+\sqrt{2}\,) &= \{3,6,10,13,17,20,23,27,30,34,37,40,44,47,51,\ldots\}.\end{aligned}$$

It's easy to calculate $\mathrm{Spec}(\sqrt{2}\,)$ with a pocket calculator, and the nth element of $\mathrm{Spec}(2+\sqrt{2}\,)$ is just $2n$ more than the nth element of $\mathrm{Spec}(\sqrt{2}\,)$, by (3.6). A closer look shows that these two spectra are also related in a much more surprising way: It seems that any number missing from one is in the other, but that no number is in both! And it's true: The positive integers are the disjoint union of $\mathrm{Spec}(\sqrt{2}\,)$ and $\mathrm{Spec}(2+\sqrt{2}\,)$. We say that these spectra form a *partition* of the positive integers.

To prove this assertion, we will count how many of the elements of $\mathrm{Spec}(\sqrt{2}\,)$ are $\leqslant n$, and how many of the elements of $\mathrm{Spec}(2+\sqrt{2}\,)$ are $\leqslant n$. If the total is n, for each n, these two spectra do indeed form a partition.

Right, because exactly one of the counts must increase when n increases by 1.

Whenever $\alpha > 0$, the number of elements in $\mathrm{Spec}(\alpha)$ that are $\leqslant n$ is

$$\begin{aligned} N(\alpha,n) &= \sum_{k>0}\bigl[\lfloor k\alpha\rfloor \leqslant n\bigr]\\ &= \sum_{k>0}\bigl[\lfloor k\alpha\rfloor < n+1\bigr]\\ &= \sum_{k>0}[k\alpha < n+1]\\ &= \sum_{k}\bigl[0<k<(n+1)/\alpha\bigr]\\ &= \lceil (n+1)/\alpha\rceil - 1\,. \end{aligned} \qquad (3.14)$$

This derivation has two special points of interest. First, it uses the law

$$m \leqslant n \quad\iff\quad m < n+1\,, \qquad \text{integers } m \text{ and } n \tag{3.15}$$

to change '$\leqslant$' to '$<$', so that the floor brackets can be removed by (3.7). Also — and this is more subtle — it sums over the range $k > 0$ instead of $k \geqslant 1$, because $(n+1)/\alpha$ might be less than 1 for certain n and α. If we had tried to apply (3.12) to determine the number of integers in $[1\,..\,(n+1)/\alpha)$, rather than the number of integers in $(0\,..\,(n+1)/\alpha)$, we would have gotten the right answer; but our derivation would have been faulty because the conditions of applicability wouldn't have been met.

Good, we have a formula for $N(\alpha, n)$. Now we can test whether or not Spec($\sqrt{2}$) and Spec($2+\sqrt{2}$) partition the positive integers, by testing whether or not $N(\sqrt{2}, n) + N(2+\sqrt{2}, n) = n$ for all integers $n > 0$, using (3.14):

$$\left\lceil \frac{n+1}{\sqrt{2}} \right\rceil - 1 + \left\lceil \frac{n+1}{2+\sqrt{2}} \right\rceil - 1 = n$$

$$\iff \quad \left\lfloor \frac{n+1}{\sqrt{2}} \right\rfloor + \left\lfloor \frac{n+1}{2+\sqrt{2}} \right\rfloor = n\,, \qquad \text{by (3.2);}$$

$$\iff \quad \frac{n+1}{\sqrt{2}} - \left\{ \frac{n+1}{\sqrt{2}} \right\} + \frac{n+1}{2+\sqrt{2}} - \left\{ \frac{n+1}{2+\sqrt{2}} \right\} = n\,, \quad \text{by (3.8).}$$

Everything simplifies now because of the neat identity

$$\frac{1}{\sqrt{2}} + \frac{1}{2+\sqrt{2}} = 1\,;$$

our condition reduces to testing whether or not

$$\left\{ \frac{n+1}{\sqrt{2}} \right\} + \left\{ \frac{n+1}{2+\sqrt{2}} \right\} = 1\,,$$

for all $n > 0$. And we win, because these are the fractional parts of two noninteger numbers that add up to the integer $n+1$. A partition it is.

3.3 FLOOR/CEILING RECURRENCES

Floors and ceilings add an interesting new dimension to the study of recurrence relations. Let's look first at the recurrence

$$\begin{aligned} K_0 &= 1\,; \\ K_{n+1} &= 1 + \min(2K_{\lfloor n/2 \rfloor}, 3K_{\lfloor n/3 \rfloor})\,, \qquad \text{for } n \geqslant 0. \end{aligned} \tag{3.16}$$

Thus, for example, K_1 is $1 + \min(2K_0, 3K_0) = 3$; the sequence begins 1, 3, 3, 4, 7, 7, 7, 9, 9, 10, 13, ... One of the authors of this book has modestly decided to call these the Knuth numbers.

Exercise 25 asks for a proof or disproof that $K_n \geqslant n$, for all $n \geqslant 0$. The first few K's just listed do satisfy the inequality, so there's a good chance that it's true in general. Let's try an induction proof: The basis $n = 0$ comes directly from the defining recurrence. For the induction step, we assume that the inequality holds for all values up through some fixed nonnegative n, and we try to show that $K_{n+1} \geqslant n + 1$. From the recurrence we know that $K_{n+1} = 1 + \min(2K_{\lfloor n/2 \rfloor}, 3K_{\lfloor n/3 \rfloor})$. The induction hypothesis tells us that $2K_{\lfloor n/2 \rfloor} \geqslant 2\lfloor n/2 \rfloor$ and $3K_{\lfloor n/3 \rfloor} \geqslant 3\lfloor n/3 \rfloor$. However, $2\lfloor n/2 \rfloor$ can be as small as $n - 1$, and $3\lfloor n/3 \rfloor$ can be as small as $n - 2$. The most we can conclude from our induction hypothesis is that $K_{n+1} \geqslant 1 + (n - 2)$; this falls far short of $K_{n+1} \geqslant n + 1$.

We now have reason to worry about the truth of $K_n \geqslant n$, so let's try to disprove it. If we can find an n such that either $2K_{\lfloor n/2 \rfloor} < n$ or $3K_{\lfloor n/3 \rfloor} < n$, or in other words such that

$$K_{\lfloor n/2 \rfloor} < n/2 \qquad \text{or} \qquad K_{\lfloor n/3 \rfloor} < n/3,$$

we will have $K_{n+1} < n + 1$. Can this be possible? We'd better not give the answer away here, because that will spoil exercise 25.

Recurrence relations involving floors and/or ceilings arise often in computer science, because algorithms based on the important technique of "divide and conquer" often reduce a problem of size n to the solution of similar problems of integer sizes that are fractions of n. For example, one way to sort n records, if $n > 1$, is to divide them into two approximately equal parts, one of size $\lceil n/2 \rceil$ and the other of size $\lfloor n/2 \rfloor$. (Notice, incidentally, that

$$n = \lceil n/2 \rceil + \lfloor n/2 \rfloor; \tag{3.17}$$

this formula comes in handy rather often.) After each part has been sorted separately (by the same method, applied recursively), we can merge the records into their final order by doing at most $n - 1$ further comparisons. Therefore the total number of comparisons performed is at most $f(n)$, where

$$\begin{aligned} f(1) &= 0; \\ f(n) &= f(\lceil n/2 \rceil) + f(\lfloor n/2 \rfloor) + n - 1, \qquad \text{for } n > 1. \end{aligned} \tag{3.18}$$

A solution to this recurrence appears in exercise 34.

The Josephus problem of Chapter 1 has a similar recurrence, which can be cast in the form

$$\begin{aligned} J(1) &= 1; \\ J(n) &= 2J(\lfloor n/2 \rfloor) - (-1)^n, \qquad \text{for } n > 1. \end{aligned}$$

We've got more tools to work with than we had in Chapter 1, so let's consider the more authentic Josephus problem in which every third person is eliminated, instead of every second. If we apply the methods that worked in Chapter 1 to this more difficult problem, we wind up with a recurrence like

$$J_3(n) \;=\; \Bigl(\Bigl\lceil \tfrac{3}{2}J_3\bigl(\lfloor\tfrac{2}{3}n\rfloor\bigr)+a_n\Bigr\rceil \bmod n\Bigr)+1\,,$$

where 'mod' is a function that we will be studying shortly, and where we have $a_n = -2$, $+1$, or $-\frac{1}{2}$ according as $n \bmod 3 = 0$, 1, or 2. But this recurrence is too horrible to pursue.

There's another approach to the Josephus problem that gives a much better setup. Whenever a person is passed over, we can assign a new number. Thus, 1 and 2 become $n+1$ and $n+2$, then 3 is executed; 4 and 5 become $n+3$ and $n+4$, then 6 is executed; ...; $3k+1$ and $3k+2$ become $n+2k+1$ and $n+2k+2$, then $3k+3$ is executed; ... then $3n$ is executed (or left to survive). For example, when $n = 10$ the numbers are

1	2	3	4	5	6	7	8	9	10
11	12		13	14		15	16		17
18			19	20			21		22
			23	24					25
			26						27
			28						
			29						
			30						

The kth person eliminated ends up with number $3k$. So we can figure out who the survivor is if we can figure out the original number of person number $3n$.

If $N > n$, person number N must have had a previous number, and we can find it as follows: We have $N = n+2k+1$ or $N = n+2k+2$, hence $k = \lfloor (N-n-1)/2 \rfloor$; the previous number was $3k+1$ or $3k+2$, respectively. That is, it was $3k + (N-n-2k) = k+N-n$. Hence we can calculate the survivor's number $J_3(n)$ as follows:

$$\begin{aligned}&N \;:=\; 3n\,;\\ &\textbf{while}\;\; N>n \;\;\textbf{do}\;\; N := \left\lfloor\frac{N-n-1}{2}\right\rfloor + N - n\,;\\ &J_3(n) \;:=\; N\,.\end{aligned}$$

This is not a closed form for $J_3(n)$; it's not even a recurrence. But at least it tells us how to calculate the answer reasonably fast, if n is large.

"Not too slow, not too fast."
—L. Armstrong

Fortunately there's a way to simplify this algorithm if we use the variable $D = 3n + 1 - N$ in place of N. (This change in notation corresponds to assigning numbers from $3n$ down to 1, instead of from 1 up to $3n$; it's sort of like a countdown.) Then the complicated assignment to N becomes

$$\begin{aligned} D \;&:=\; 3n+1-\left(\left\lfloor\frac{(3n+1-D)-n-1}{2}\right\rfloor + (3n+1-D)-n\right) \\ &=\; n+D-\left\lfloor\frac{2n-D}{2}\right\rfloor \;=\; D-\left\lfloor\frac{-D}{2}\right\rfloor \;=\; D+\left\lceil\frac{D}{2}\right\rceil \;=\; \left\lceil\tfrac{3}{2}D\right\rceil, \end{aligned}$$

and we can rewrite the algorithm as follows:

$$\begin{aligned} &D \;:=\; 1\,; \\ &\textbf{while}\;\; D \leqslant 2n \;\;\textbf{do}\;\; D := \left\lceil\tfrac{3}{2}D\right\rceil; \\ &J_3(n) \;:=\; 3n+1-D\,. \end{aligned}$$

Aha! This looks much nicer, because n enters the calculation in a very simple way. In fact, we can show by the same reasoning that the survivor $J_q(n)$ when every qth person is eliminated can be calculated as follows:

$$\begin{aligned} &D \;:=\; 1\,; \\ &\textbf{while}\;\; D \leqslant (q-1)n \;\;\textbf{do}\;\; D := \left\lceil\tfrac{q}{q-1}D\right\rceil; \\ &J_q(n) \;:=\; qn+1-D\,. \end{aligned} \tag{3.19}$$

In the case $q = 2$ that we know so well, this makes D grow to 2^{m+1} when $n = 2^m + l$; hence $J_2(n) = 2(2^m + l) + 1 - 2^{m+1} = 2l + 1$. Good.

The recipe in (3.19) computes a sequence of integers that can be defined by the following recurrence:

$$\begin{aligned} D_0^{(q)} &= 1\,; \\ D_n^{(q)} &= \left\lceil\frac{q}{q-1}D_{n-1}^{(q)}\right\rceil \qquad \text{for } n > 0. \end{aligned} \tag{3.20}$$

These numbers don't seem to relate to any familiar functions in a simple way, except when $q = 2$; hence they probably don't have a nice closed form. But if we're willing to accept the sequence $D_n^{(q)}$ as "known," then it's easy to describe the solution to the generalized Josephus problem: The survivor $J_q(n)$ is $qn + 1 - D_k^{(q)}$, where k is as small as possible such that $D_k^{(q)} > (q-1)n$.

"Known" like, say, harmonic numbers. A. M. Odlyzko and H. S. Wilf have shown [283] that $D_n^{(3)} = \lfloor(\tfrac{3}{2})^n C\rfloor$, *where* $C \approx 1.622270503$.

3.4 'MOD': THE BINARY OPERATION

The quotient of n divided by m is $\lfloor n/m \rfloor$, when m and n are positive integers. It's handy to have a simple notation also for the remainder of this division, and we call it '$n \bmod m$'. The basic formula

$$n = m\underbrace{\lfloor n/m \rfloor}_{\text{quotient}} + \underbrace{n \bmod m}_{\text{remainder}}$$

tells us that we can express $n \bmod m$ as $n - m\lfloor n/m \rfloor$. We can generalize this to negative integers, and in fact to arbitrary real numbers:

$$x \bmod y = x - y\lfloor x/y \rfloor, \qquad \text{for } y \neq 0. \tag{3.21}$$

This defines 'mod' as a binary operation, just as addition and subtraction are binary operations. Mathematicians have used mod this way informally for a long time, taking various quantities mod 10, mod 2π, and so on, but only in the last twenty years has it caught on formally. Old notion, new notation.

Why do they call it 'mod': The Binary Operation? Stay tuned to find out in the next, exciting, chapter!

We can easily grasp the intuitive meaning of $x \bmod y$, when x and y are positive real numbers, if we imagine a circle of circumference y whose points have been assigned real numbers in the interval $[0\,..\,y)$. If we travel a distance x around the circle, starting at 0, we end up at $x \bmod y$. (And the number of times we encounter 0 as we go is $\lfloor x/y \rfloor$.)

When x or y is negative, we need to look at the definition carefully in order to see exactly what it means. Here are some integer-valued examples:

Beware of computer languages that use another definition.

$$\begin{aligned} 5 \bmod 3 &= 5 - 3\lfloor 5/3 \rfloor &&= 2; \\ 5 \bmod -3 &= 5 - (-3)\lfloor 5/(-3) \rfloor &&= -1; \\ -5 \bmod 3 &= -5 - 3\lfloor -5/3 \rfloor &&= 1; \\ -5 \bmod -3 &= -5 - (-3)\lfloor -5/(-3) \rfloor &&= -2. \end{aligned}$$

The number after 'mod' is called the *modulus*; nobody has yet decided what to call the number before 'mod'. In applications, the modulus is usually positive, but the definition makes perfect sense when the modulus is negative. In both cases the value of $x \bmod y$ is between 0 and the modulus:

How about calling the other number the modumor?

$$\begin{aligned} 0 &\leqslant x \bmod y < y, &&\text{for } y > 0; \\ 0 &\geqslant x \bmod y > y, &&\text{for } y < 0. \end{aligned}$$

What about $y = 0$? Definition (3.21) leaves this case undefined, in order to avoid division by zero, but to be complete we can define

$$x \bmod 0 = x. \tag{3.22}$$

This convention preserves the property that $x \bmod y$ always differs from x by a multiple of y. (It might seem more natural to make the function continuous at 0, by defining $x \bmod 0 = \lim_{y \to 0} x \bmod y = 0$. But we'll see in Chapter 4 that this would be much less useful. Continuity is not an important aspect of the mod operation.)

We've already seen one special case of mod in disguise, when we wrote x in terms of its integer and fractional parts, $x = \lfloor x \rfloor + \{x\}$. The fractional part can also be written $x \bmod 1$, because we have

$$x = \lfloor x \rfloor + x \bmod 1 .$$

Notice that parentheses aren't needed in this formula; we take mod to bind more tightly than addition or subtraction.

The floor function has been used to define mod, and the ceiling function hasn't gotten equal time. We could perhaps use the ceiling to define a mod analog like

$$x \text{ mumble } y = y\lceil x/y \rceil - x ;$$

There was a time in the 70s when 'mod' was the fashion. Maybe the new mumble function should be called 'punk'?

No—I like 'mumble'.

Notice that x mumble $y = (-x) \bmod y$.

in our circle analogy this represents the distance the traveler needs to continue, after going a distance x, to get back to the starting point 0. But of course we'd need a better name than 'mumble'. If sufficient applications come along, an appropriate name will probably suggest itself.

The distributive law is mod's most important algebraic property: We have

$$c(x \bmod y) = (cx) \bmod (cy) \tag{3.23}$$

for all real c, x, and y. (Those who like mod to bind less tightly than multiplication may remove the parentheses from the right side here, too.) It's easy to prove this law from definition (3.21), since

$$c(x \bmod y) = c(x - y\lfloor x/y \rfloor) = cx - cy\lfloor cx/cy \rfloor = cx \bmod cy ,$$

if $cy \neq 0$; and the zero-modulus cases are trivially true. Our four examples using ± 5 and ± 3 illustrate this law twice, with $c = -1$. An identity like (3.23) is reassuring, because it gives us reason to believe that 'mod' has not been defined improperly.

The remainder, eh?

In the remainder of this section, we'll consider an application in which 'mod' turns out to be helpful although it doesn't play a central role. The problem arises frequently in a variety of situations: We want to partition n things into m groups as equally as possible.

Suppose, for example, that we have n short lines of text that we'd like to arrange in m columns. For æsthetic reasons, we want the columns to be arranged in decreasing order of length (actually nonincreasing order); and the lengths should be approximately the same—no two columns should differ by more than one line's worth of text. If 37 lines of text are being divided into five columns, we would therefore prefer the arrangement on the right:

8	8	8	8	5
line 1	line 9	line 17	line 25	line 33
line 2	line 10	line 18	line 26	line 34
line 3	line 11	line 19	line 27	line 35
line 4	line 12	line 20	line 28	line 36
line 5	line 13	line 21	line 29	line 37
line 6	line 14	line 22	line 30	
line 7	line 15	line 23	line 31	
line 8	line 16	line 24	line 32	

8	8	7	7	7
line 1	line 9	line 17	line 24	line 31
line 2	line 10	line 18	line 25	line 32
line 3	line 11	line 19	line 26	line 33
line 4	line 12	line 20	line 27	line 34
line 5	line 13	line 21	line 28	line 35
line 6	line 14	line 22	line 29	line 36
line 7	line 15	line 23	line 30	line 37
line 8	line 16			

Furthermore we want to distribute the lines of text columnwise — first deciding how many lines go into the first column and then moving on to the second, the third, and so on — because that's the way people read. Distributing row by row would give us the correct number of lines in each column, but the ordering would be wrong. (We would get something like the arrangement on the right, but column 1 would contain lines 1, 6, 11, ..., 36, instead of lines 1, 2, 3, ..., 8 as desired.)

A row-by-row distribution strategy can't be used, but it does tell us how many lines to put in each column. If n is not a multiple of m, the row-by-row procedure makes it clear that the long columns should each contain $\lceil n/m \rceil$ lines, and the short columns should each contain $\lfloor n/m \rfloor$. There will be exactly $n \bmod m$ long columns (and, as it turns out, there will be exactly n mumble m short ones).

Let's generalize the terminology and talk about 'things' and 'groups' instead of 'lines' and 'columns'. We have just decided that the first group should contain $\lceil n/m \rceil$ things; therefore the following sequential distribution scheme ought to work: To distribute n things into m groups, when $m > 0$, put $\lceil n/m \rceil$ things into one group, then use the same procedure recursively to put the remaining $n' = n - \lceil n/m \rceil$ things into $m' = m - 1$ additional groups.

For example, if $n = 314$ and $m = 6$, the distribution goes like this:

remaining things	remaining groups	⌈things/groups⌉
314	6	53
261	5	53
208	4	52
156	3	52
104	2	52
52	1	52

It works. We get groups of approximately the same size, even though the divisor keeps changing.

Why does it work? In general we can suppose that $n = qm + r$, where $q = \lfloor n/m \rfloor$ and $r = n \bmod m$. The process is simple if $r = 0$: We put $\lceil n/m \rceil = q$ things into the first group and replace n by $n' = n - q$, leaving

$n' = qm'$ things to put into the remaining $m' = m - 1$ groups. And if $r > 0$, we put $\lceil n/m \rceil = q + 1$ things into the first group and replace n by $n' = n - q - 1$, leaving $n' = qm' + r - 1$ things for subsequent groups. The new remainder is $r' = r - 1$, but q stays the same. It follows that there will be r groups with $q + 1$ things, followed by $m - r$ groups with q things.

How many things are in the kth group? We'd like a formula that gives $\lceil n/m \rceil$ when $k \leqslant n \bmod m$, and $\lfloor n/m \rfloor$ otherwise. It's not hard to verify that

$$\left\lceil \frac{n-k+1}{m} \right\rceil$$

has the desired properties, because this reduces to $q + \lceil (r-k+1)/m \rceil$ if we write $n = qm + r$ as in the preceding paragraph; here $q = \lfloor n/m \rfloor$. We have $\lceil (r-k+1)/m \rceil = [k \leqslant r]$, if $1 \leqslant k \leqslant m$ and $0 \leqslant r < m$. Therefore we can write an identity that expresses the partition of n into m as-equal-as-possible parts in nonincreasing order:

$$n = \left\lceil \frac{n}{m} \right\rceil + \left\lceil \frac{n-1}{m} \right\rceil + \cdots + \left\lceil \frac{n-m+1}{m} \right\rceil . \qquad (3.24)$$

This identity is valid for all positive integers m, and for all integers n (whether positive, negative, or zero). We have already encountered the case $m = 2$ in (3.17), although we wrote it in a slightly different form, $n = \lceil n/2 \rceil + \lfloor n/2 \rfloor$.

If we had wanted the parts to be in nondecreasing order, with the small groups coming before the larger ones, we could have proceeded in the same way but with $\lfloor n/m \rfloor$ things in the first group. Then we would have derived the corresponding identity

$$n = \left\lfloor \frac{n}{m} \right\rfloor + \left\lfloor \frac{n+1}{m} \right\rfloor + \cdots + \left\lfloor \frac{n+m-1}{m} \right\rfloor . \qquad (3.25)$$

It's possible to convert between (3.25) and (3.24) by using either (3.4) or the identity of exercise 12.

Some claim that it's too dangerous to replace anything by an mx.

Now if we replace n in (3.25) by $\lfloor mx \rfloor$, and apply rule (3.11) to remove floors inside of floors, we get an identity that holds for all real x:

$$\lfloor mx \rfloor = \lfloor x \rfloor + \left\lfloor x + \frac{1}{m} \right\rfloor + \cdots + \left\lfloor x + \frac{m-1}{m} \right\rfloor . \qquad (3.26)$$

This is rather amazing, because the floor function is an integer approximation of a real value, but the single approximation on the left equals the sum of a bunch of them on the right. If we assume that $\lfloor x \rfloor$ is roughly $x - \frac{1}{2}$ on the average, the left-hand side is roughly $mx - \frac{1}{2}$, while the right-hand side comes to roughly $(x - \frac{1}{2}) + (x - \frac{1}{2} + \frac{1}{m}) + \cdots + (x - \frac{1}{2} + \frac{m-1}{m}) = mx - \frac{1}{2}$; the sum of all these rough approximations turns out to be exact!

3.5 FLOOR/CEILING SUMS

Equation (3.26) demonstrates that it's possible to get a closed form for at least one kind of sum that involves $\lfloor\ \rfloor$. Are there others? Yes. The trick that usually works in such cases is to get rid of the floor or ceiling by introducing a new variable.

For example, let's see if it's possible to do the sum

$$\sum_{0\leqslant k<n} \lfloor\sqrt{k}\rfloor$$

in closed form. One idea is to introduce the variable $m = \lfloor\sqrt{k}\rfloor$; we can do this "mechanically" by proceeding as we did in the roulette problem:

$$\begin{aligned}\sum_{0\leqslant k<n} \lfloor\sqrt{k}\rfloor &= \sum_{k,m\geqslant 0} m[k<n]\bigl[m=\lfloor\sqrt{k}\rfloor\bigr]\\ &= \sum_{k,m\geqslant 0} m[k<n]\bigl[m\leqslant\sqrt{k}<m+1\bigr]\\ &= \sum_{k,m\geqslant 0} m[k<n]\bigl[m^2\leqslant k<(m+1)^2\bigr]\\ &= \sum_{k,m\geqslant 0} m\bigl[m^2\leqslant k<(m+1)^2\leqslant n\bigr]\\ &\qquad + \sum_{k,m\geqslant 0} m\bigl[m^2\leqslant k<n<(m+1)^2\bigr]\,.\end{aligned}$$

Once again the boundary conditions are a bit delicate. Let's assume first that $n = a^2$ is a perfect square. Then the second sum is zero, and the first can be evaluated by our usual routine:

$$\begin{aligned}&\sum_{k,m\geqslant 0} m\bigl[m^2\leqslant k<(m+1)^2\leqslant a^2\bigr]\\ &\quad= \sum_{m\geqslant 0} m\bigl((m+1)^2-m^2\bigr)[m+1\leqslant a]\\ &\quad= \sum_{m\geqslant 0} m(2m+1)[m<a]\\ &\quad= \sum_{m\geqslant 0} (2m^{\underline{2}}+3m^{\underline{1}})[m<a]\\ &\quad= \textstyle\sum_0^a (2m^{\underline{2}}+3m^{\underline{1}})\,\delta m\\ &\quad= \tfrac{2}{3}a(a-1)(a-2)+\tfrac{3}{2}a(a-1) \;=\; \tfrac{1}{6}(4a+1)a(a-1)\,.\end{aligned}$$

Falling powers make the sum come tumbling down.

In the general case we can let $a = \lfloor\sqrt{n}\rfloor$; then we merely need to add the terms for $a^2 \leqslant k < n$, which are all equal to a, so they sum to $(n-a^2)a$. This gives the desired closed form,

$$\sum_{0\leqslant k<n} \lfloor\sqrt{k}\rfloor \;=\; na - \tfrac{1}{3}a^3 - \tfrac{1}{2}a^2 - \tfrac{1}{6}a\,, \qquad a = \lfloor\sqrt{n}\rfloor. \tag{3.27}$$

Another approach to such sums is to replace an expression of the form $\lfloor x\rfloor$ by $\sum_j [1\leqslant j\leqslant x]$; this is legal whenever $x \geqslant 0$. Here's how that method works in the sum of $\lfloor$square roots$\rfloor$, if we assume for convenience that $n = a^2$:

$$\begin{aligned}\sum_{0\leqslant k<a^2} \lfloor\sqrt{k}\rfloor \;&=\; \sum_{j,k} [1\leqslant j\leqslant \sqrt{k}\,][0\leqslant k<a^2]\\ &=\; \sum_{1\leqslant j<a}\;\sum_k [j^2\leqslant k<a^2]\\ &=\; \sum_{1\leqslant j<a} (a^2-j^2) \;=\; a^3 - \tfrac{1}{3}a(a+\tfrac{1}{2})(a+1)\,, \quad \text{integer } a.\end{aligned}$$

Now here's another example where a change of variable leads to a transformed sum. A remarkable theorem was discovered independently by three mathematicians — Bohl [34], Sierpiński [326], and Weyl [368] — at about the same time in 1909: If α is irrational then the fractional parts $\{n\alpha\}$ are very uniformly distributed between 0 and 1, as $n \to \infty$. One way to state this is that

$$\lim_{n\to\infty} \frac{1}{n} \sum_{0\leqslant k<n} f\bigl(\{k\alpha\}\bigr) \;=\; \int_0^1 f(x)\,dx \tag{3.28}$$

for all irrational α and all bounded functions f that are continuous almost everywhere. For example, the *average* value of $\{n\alpha\}$ can be found by setting $f(x) = x$; we get $\frac{1}{2}$. (That's exactly what we might expect; but it's nice to know that it is really, provably true, no matter how irrational α is.)

Warning: This stuff is fairly advanced. Better skim the next two pages on first reading; they aren't crucial.
— Friendly TA

The theorem of Bohl, Sierpiński, and Weyl is proved by approximating $f(x)$ above and below by "step functions," which are linear combinations of the simple functions

$$f_v(x) \;=\; [0\leqslant x<v]$$

when $0 \leqslant v \leqslant 1$. Our purpose here is not to prove the theorem; that's a job for calculus books. But let's try to figure out the basic reason why it holds, by seeing how well it works in the special case $f(x) = f_v(x)$. In other words, let's try to see how close the sum

Start Skimming

$$\sum_{0\leqslant k<n} \bigl[\{k\alpha\}<v\bigr]$$

gets to the "ideal" value nv, when n is large and α is irrational.

For this purpose we define the *discrepancy* $D(\alpha, n)$ to be the maximum absolute value, over all $0 \leqslant v \leqslant 1$, of the sum

$$s(\alpha, n, v) \;=\; \sum_{0\leqslant k<n} \Bigl(\bigl[\{k\alpha\}<v\bigr] - v\Bigr)\,. \qquad (3.29)$$

Our goal is to show that $D(\alpha, n)$ is "not too large" when compared with n, by showing that $|s(\alpha, n, v)|$ is always reasonably small when α is irrational. We can assume without loss of generality that $0 < \alpha < 1$.

First we can rewrite $s(\alpha, n, v)$ in simpler form, then introduce a new index variable j:

$$\begin{aligned}
\sum_{0\leqslant k<n} \Bigl(\bigl[\{k\alpha\}<v\bigr] - v\Bigr) \;&=\; \sum_{0\leqslant k<n} \bigl(\lfloor k\alpha\rfloor - \lfloor k\alpha - v\rfloor - v\bigr) \\
&=\; -nv + \sum_{0\leqslant k<n}\,\sum_{j} \bigl[k\alpha - v < j \leqslant k\alpha\bigr] \\
&=\; -nv + \sum_{0\leqslant j<\lceil n\alpha\rceil}\,\sum_{k<n} \bigl[j\alpha^{-1} \leqslant k < (j+v)\alpha^{-1}\bigr]\,.
\end{aligned}$$

If we're lucky, we can do the sum on k. But we ought to introduce some new variables, so that the formula won't be such a mess. Let us write

Right, name and conquer.
The change of variable from k to j is the main point.
—Friendly TA

$$\begin{aligned}
a \;&=\; \lfloor \alpha^{-1}\rfloor\,, &\qquad \alpha^{-1} \;&=\; a + \alpha'\,; \\
b \;&=\; \lceil v\alpha^{-1}\rceil\,, &\qquad v\alpha^{-1} \;&=\; b - v'\,.
\end{aligned}$$

Thus $\alpha' = \{\alpha^{-1}\}$ is the fractional part of α^{-1}, and v' is the mumble-fractional part of $v\alpha^{-1}$.

Once again the boundary conditions are our only source of grief. For now, let's forget the restriction '$k < n$' and evaluate the sum on k without it:

$$\begin{aligned}
\sum_{k} \Bigl[k \in \bigl[j\alpha^{-1} \mathinner{\ldotp\ldotp} (j+v)\alpha^{-1}\bigr)\Bigr] \;&=\; \bigl\lceil (j+v)(a+\alpha')\bigr\rceil - \bigl\lceil j(a+\alpha')\bigr\rceil \\
&=\; b + \lceil j\alpha' - v'\rceil - \lceil j\alpha'\rceil\,.
\end{aligned}$$

OK, that's pretty simple; we plug it in and plug away:

$$s(\alpha, n, v) \;=\; -nv + \lceil n\alpha\rceil b + \sum_{0\leqslant j<\lceil n\alpha\rceil} \bigl(\lceil j\alpha' - v'\rceil - \lceil j\alpha'\rceil\bigr) - S\,, \qquad (3.30)$$

where S is a correction for the cases with $k \geqslant n$ that we have failed to exclude. The quantity $j\alpha'$ will be an integer only when $j = 0$, since α (hence α') is irrational; and $j\alpha' - v'$ will be an integer for at most one value of j. So we can change the ceiling terms to floors:

$$s(\alpha,n,v) \;=\; -nv + \lceil n\alpha \rceil b - \sum_{0\leqslant j<\lceil n\alpha\rceil} \bigl(\lfloor j\alpha' \rfloor - \lfloor j\alpha' - v' \rfloor\bigr) - S + \{0 \text{ or } 1\}.$$

(The formula $\{0$ or $1\}$ stands for something that's either 0 or 1; we needn't commit ourselves, because the details don't really matter.)

Interesting. Instead of a closed form, we're getting a sum that looks rather like $s(\alpha,n,v)$ but with different parameters: α' instead of α, $\lceil n\alpha\rceil$ instead of n, and v' instead of v. So we'll have a recurrence for $s(\alpha,n,v)$, which (hopefully) will lead to a recurrence for the discrepancy $D(\alpha,n)$. This means we want to get

$$s(\alpha',\lceil n\alpha\rceil,v') \;=\; \sum_{0\leqslant j<\lceil n\alpha\rceil} \bigl(\lfloor j\alpha' \rfloor - \lfloor j\alpha' - v' \rfloor - v'\bigr)$$

into the act:

$$s(\alpha,n,v) \;=\; -nv + \lceil n\alpha\rceil b - \lceil n\alpha\rceil v' - s(\alpha',\lceil n\alpha\rceil,v') - S + \{0 \text{ or } 1\}.$$

Recalling that $b - v' = v\alpha^{-1}$, we see that everything will simplify beautifully if we replace $\lceil n\alpha\rceil(b-v')$ by $n\alpha(b-v') = nv$:

$$s(\alpha,n,v) \;=\; -s(\alpha',\lceil n\alpha\rceil,v') - S + \epsilon + \{0 \text{ or } 1\}.$$

Here ϵ is a positive error less than $v\alpha^{-1}$. Exercise 18 proves that S is, similarly, between 0 and $\lceil v\alpha^{-1}\rceil$. And we can remove the term for $j = \lceil n\alpha\rceil - 1 = \lfloor n\alpha\rfloor$ from the sum, since it contributes either v' or $v'-1$. Hence, if we take the maximum of absolute values over all v, we get

$$D(\alpha,n) \;\leqslant\; D(\alpha',\lfloor\alpha n\rfloor) + \alpha^{-1} + 2\,. \tag{3.31}$$

The methods we'll learn in succeeding chapters will allow us to conclude from this recurrence that $D(\alpha,n)$ is always much smaller than n, when n is sufficiently large. Hence theorem (3.28) is true; however, convergence to the limit is not always very fast. (See exercises 9.45 and 9.61.)

Stop Skimming

Whew; that was quite an exercise in manipulation of sums, floors, and ceilings. Readers who are not accustomed to "proving that errors are small" might find it hard to believe that anybody would have the courage to keep going, when faced with such weird-looking sums. But actually, a second look shows that there's a simple motivating thread running through the whole calculation. The main idea is that a certain sum $s(\alpha,n,v)$ of n terms can be reduced to a similar sum of at most $\lceil\alpha n\rceil$ terms. Everything else cancels out except for a small residual left over from terms near the boundaries.

Let's take a deep breath now and do one more sum, which is not trivial but has the great advantage (compared with what we've just been doing) that it comes out in closed form so that we can easily check the answer. Our goal now will be to generalize the sum in (3.26) by finding an expression for

$$\sum_{0 \leqslant k < m} \left\lfloor \frac{nk + x}{m} \right\rfloor, \qquad \text{integer } m > 0, \quad \text{integer } n.$$

Is this a harder sum of floors, or a sum of harder floors?

Finding a closed form for this sum is tougher than what we've done so far (except perhaps for the discrepancy problem we just looked at). But it's instructive, so we'll hack away at it for the rest of this chapter.

Be forewarned: This is the beginning of a pattern, in that the last part of the chapter consists of the solution of some long, difficult problem, with little more motivation than curiosity.
—Students

As usual, especially with tough problems, we start by looking at small cases. The special case $n = 1$ is (3.26), with x replaced by x/m:

$$\left\lfloor \frac{x}{m} \right\rfloor + \left\lfloor \frac{1+x}{m} \right\rfloor + \cdots + \left\lfloor \frac{m-1+x}{m} \right\rfloor = \lfloor x \rfloor .$$

And as in Chapter 1, we find it useful to get more data by generalizing downwards to the case $n = 0$:

$$\left\lfloor \frac{x}{m} \right\rfloor + \left\lfloor \frac{x}{m} \right\rfloor + \cdots + \left\lfloor \frac{x}{m} \right\rfloor = m \left\lfloor \frac{x}{m} \right\rfloor .$$

Touché. But c'mon, gang, do you always need to be told about applications before you can get interested in something? This sum arises, for example, in the study of random number generation and testing. But mathematicians looked at it long before computers came along, because they found it natural to ask if there's a way to sum arithmetic progressions that have been "floored."
—Your instructor

Our problem has two parameters, m and n; let's look at some small cases for m. When $m = 1$ there's just a single term in the sum and its value is $\lfloor x \rfloor$. When $m = 2$ the sum is $\lfloor x/2 \rfloor + \lfloor (x+n)/2 \rfloor$. We can remove the interaction between x and n by removing n from inside the floor function, but to do that we must consider even and odd n separately. If n is even, $n/2$ is an integer, so we can remove it from the floor:

$$\left\lfloor \frac{x}{2} \right\rfloor + \left(\left\lfloor \frac{x}{2} \right\rfloor + \frac{n}{2} \right) = 2 \left\lfloor \frac{x}{2} \right\rfloor + \frac{n}{2} .$$

If n is odd, $(n-1)/2$ is an integer so we get

$$\left\lfloor \frac{x}{2} \right\rfloor + \left(\left\lfloor \frac{x+1}{2} \right\rfloor + \frac{n-1}{2} \right) = \lfloor x \rfloor + \frac{n-1}{2} .$$

The last step follows from (3.26) with $m = 2$.

These formulas for even and odd n slightly resemble those for $n = 0$ and 1, but no clear pattern has emerged yet; so we had better continue exploring some more small cases. For $m = 3$ the sum is

$$\left\lfloor \frac{x}{3} \right\rfloor + \left\lfloor \frac{x+n}{3} \right\rfloor + \left\lfloor \frac{x+2n}{3} \right\rfloor ,$$

and we consider three cases for n: Either it's a multiple of 3, or it's 1 more than a multiple, or it's 2 more. That is, $n \bmod 3 = 0$, 1, or 2. If $n \bmod 3 = 0$

then $n/3$ and $2n/3$ are integers, so the sum is

$$\left\lfloor\frac{x}{3}\right\rfloor + \left(\left\lfloor\frac{x}{3}\right\rfloor + \frac{n}{3}\right) + \left(\left\lfloor\frac{x}{3}\right\rfloor + \frac{2n}{3}\right) = 3\left\lfloor\frac{x}{3}\right\rfloor + n\,.$$

If $n \bmod 3 = 1$ then $(n-1)/3$ and $(2n-2)/3$ are integers, so we have

$$\left\lfloor\frac{x}{3}\right\rfloor + \left(\left\lfloor\frac{x+1}{3}\right\rfloor + \frac{n-1}{3}\right) + \left(\left\lfloor\frac{x+2}{3}\right\rfloor + \frac{2n-2}{3}\right) = \lfloor x\rfloor + n - 1\,.$$

Again this last step follows from (3.26), this time with $m = 3$. And finally, if $n \bmod 3 = 2$ then

$$\left\lfloor\frac{x}{3}\right\rfloor + \left(\left\lfloor\frac{x+2}{3}\right\rfloor + \frac{n-2}{3}\right) + \left(\left\lfloor\frac{x+1}{3}\right\rfloor + \frac{2n-1}{3}\right) = \lfloor x\rfloor + n - 1\,.$$

"Inventive genius requires pleasurable mental activity as a condition for its vigorous exercise. 'Necessity is the mother of invention' is a silly proverb. 'Necessity is the mother of futile dodges' is much nearer to the truth. The basis of the growth of modern invention is science, and science is almost wholly the outgrowth of pleasurable intellectual curiosity."
—A. N. Whitehead [371]

The left hemispheres of our brains have finished the case $m = 3$, but the right hemispheres still can't recognize the pattern, so we proceed to $m = 4$:

$$\left\lfloor\frac{x}{4}\right\rfloor + \left\lfloor\frac{x+n}{4}\right\rfloor + \left\lfloor\frac{x+2n}{4}\right\rfloor + \left\lfloor\frac{x+3n}{4}\right\rfloor\,.$$

At least we know enough by now to consider cases based on $n \bmod m$. If $n \bmod 4 = 0$ then

$$\left\lfloor\frac{x}{4}\right\rfloor + \left(\left\lfloor\frac{x}{4}\right\rfloor + \frac{n}{4}\right) + \left(\left\lfloor\frac{x}{4}\right\rfloor + \frac{2n}{4}\right) + \left(\left\lfloor\frac{x}{4}\right\rfloor + \frac{3n}{4}\right) = 4\left\lfloor\frac{x}{4}\right\rfloor + \frac{3n}{2}\,.$$

And if $n \bmod 4 = 1$,

$$\left\lfloor\frac{x}{4}\right\rfloor + \left(\left\lfloor\frac{x+1}{4}\right\rfloor + \frac{n-1}{4}\right) + \left(\left\lfloor\frac{x+2}{4}\right\rfloor + \frac{2n-2}{4}\right) + \left(\left\lfloor\frac{x+3}{4}\right\rfloor + \frac{3n-3}{4}\right)$$
$$= \lfloor x\rfloor + \frac{3n}{2} - \frac{3}{2}\,.$$

The case $n \bmod 4 = 3$ turns out to give the same answer. Finally, in the case $n \bmod 4 = 2$ we get something a bit different, and this turns out to be an important clue to the behavior in general:

$$\left\lfloor\frac{x}{4}\right\rfloor + \left(\left\lfloor\frac{x+2}{4}\right\rfloor + \frac{n-2}{4}\right) + \left(\left\lfloor\frac{x}{4}\right\rfloor + \frac{2n}{4}\right) + \left(\left\lfloor\frac{x+2}{4}\right\rfloor + \frac{3n-2}{4}\right)$$
$$= 2\left(\left\lfloor\frac{x}{4}\right\rfloor + \left\lfloor\frac{x+2}{4}\right\rfloor\right) + \frac{3n}{2} - 1 = 2\left\lfloor\frac{x}{2}\right\rfloor + \frac{3n}{2} - 1\,.$$

This last step simplifies something of the form $\lfloor y/2\rfloor + \lfloor (y+1)/2\rfloor$, which again is a special case of (3.26).

To summarize, here's the value of our sum for small m:

m	$n \bmod m = 0$	$n \bmod m = 1$	$n \bmod m = 2$	$n \bmod m = 3$
1	$\lfloor x \rfloor$			
2	$2\left\lfloor \frac{x}{2} \right\rfloor + \frac{n}{2}$	$\lfloor x \rfloor + \frac{n}{2} - \frac{1}{2}$		
3	$3\left\lfloor \frac{x}{3} \right\rfloor + n$	$\lfloor x \rfloor + n - 1$	$\lfloor x \rfloor + n - 1$	
4	$4\left\lfloor \frac{x}{4} \right\rfloor + \frac{3n}{2}$	$\lfloor x \rfloor + \frac{3n}{2} - \frac{3}{2}$	$2\left\lfloor \frac{x}{2} \right\rfloor + \frac{3n}{2} - 1$	$\lfloor x \rfloor + \frac{3n}{2} - \frac{3}{2}$

It looks as if we're getting something of the form

$$a\left\lfloor \frac{x}{a} \right\rfloor + bn + c\,,$$

where a, b, and c somehow depend on m and n. Even the myopic among us can see that b is probably $(m-1)/2$. It's harder to discern an expression for a; but the case $n \bmod 4 = 2$ gives us a hint that a is probably $\gcd(m,n)$, the greatest common divisor of m and n. This makes sense because $\gcd(m,n)$ is the factor we remove from m and n when reducing the fraction n/m to lowest terms, and our sum involves the fraction n/m. (We'll look carefully at gcd operations in Chapter 4.) The value of c seems more mysterious, but perhaps it will drop out of our proofs for a and b.

In computing the sum for small m, we've effectively rewritten each term of the sum as

$$\left\lfloor \frac{x+kn}{m} \right\rfloor = \left\lfloor \frac{x + kn \bmod m}{m} \right\rfloor + \frac{kn}{m} - \frac{kn \bmod m}{m}\,,$$

because $(kn - kn \bmod m)/m$ is an integer that can be removed from inside the floor brackets. Thus the original sum can be expanded into the following tableau:

$$\begin{array}{rcccccc}
 & \left\lfloor \frac{x}{m} \right\rfloor & + & \frac{0}{m} & - & \frac{0 \bmod m}{m} \\
+ & \left\lfloor \frac{x + n \bmod m}{m} \right\rfloor & + & \frac{n}{m} & - & \frac{n \bmod m}{m} \\
+ & \left\lfloor \frac{x + 2n \bmod m}{m} \right\rfloor & + & \frac{2n}{m} & - & \frac{2n \bmod m}{m} \\
 & \vdots & & \vdots & & \vdots \\
+ & \left\lfloor \frac{x + (m-1)n \bmod m}{m} \right\rfloor & + & \frac{(m-1)n}{m} & - & \frac{(m-1)n \bmod m}{m}\,.
\end{array}$$

When we experimented with small values of m, these three columns led respectively to $a\lfloor x/a\rfloor$, bn, and c.

In particular, we can see how b arises. The second column is an arithmetic progression, whose sum we know — it's the average of the first and last terms, times the number of terms:

$$\frac{1}{2}\left(0+\frac{(m-1)n}{m}\right)\cdot m \;=\; \frac{(m-1)n}{2}\,.$$

So our guess that $b=(m-1)/2$ has been verified.

The first and third columns seem tougher; to determine a and c we must take a closer look at the sequence of numbers

$$0 \bmod m,\quad n \bmod m,\quad 2n \bmod m,\quad \ldots,\quad (m-1)n \bmod m.$$

Suppose, for example, that $m=12$ and $n=5$. If we think of the sequence as times on a clock, the numbers are 0 o'clock (we take 12 o'clock to be 0 o'clock), then 5 o'clock, 10 o'clock, 3 o'clock (= 15 o'clock), 8 o'clock, and so on. It turns out that we hit every hour exactly once.

Now suppose $m=12$ and $n=8$. The numbers are 0 o'clock, 8 o'clock, 4 o'clock (= 16 o'clock), but then 0, 8, and 4 repeat. Since both 8 and 12 are multiples of 4, and since the numbers start at 0 (also a multiple of 4), there's no way to break out of this pattern — they must all be multiples of 4.

Lemma now, dilemma later.

In these two cases we have $\gcd(12,5)=1$ and $\gcd(12,8)=4$. The general rule, which we will prove next chapter, states that if $d=\gcd(m,n)$ then we get the numbers 0, d, $2d$, $\ldots$, $m-d$ in some order, followed by $d-1$ more copies of the same sequence. For example, with $m=12$ and $n=8$ the pattern 0, 8, 4 occurs four times.

The first column of our sum now makes complete sense. It contains d copies of the terms $\lfloor x/m\rfloor$, $\lfloor (x+d)/m\rfloor$, $\ldots$, $\lfloor (x+m-d)/m\rfloor$, in some order, so its sum is

$$\begin{aligned} &d\left(\left\lfloor\frac{x}{m}\right\rfloor+\left\lfloor\frac{x+d}{m}\right\rfloor+\cdots+\left\lfloor\frac{x+m-d}{m}\right\rfloor\right)\\ &\qquad= d\left(\left\lfloor\frac{x/d}{m/d}\right\rfloor+\left\lfloor\frac{x/d+1}{m/d}\right\rfloor+\cdots+\left\lfloor\frac{x/d+m/d-1}{m/d}\right\rfloor\right)\\ &\qquad= d\left\lfloor\frac{x}{d}\right\rfloor\,. \end{aligned}$$

This last step is yet another application of (3.26). Our guess for a has been verified:

$$a \;=\; d \;=\; \gcd(m,n)\,.$$

Also, as we guessed, we can now compute c, because the third column has become easy to fathom. It contains d copies of the arithmetic progression $0/m$, d/m, $2d/m$, $\ldots$, $(m-d)/m$, so its sum is

$$d\left(\frac{1}{2}\left(0+\frac{m-d}{m}\right)\cdot\frac{m}{d}\right) = \frac{m-d}{2};$$

the third column is actually subtracted, not added, so we have

$$c = \frac{d-m}{2}.$$

End of mystery, end of quest. The desired closed form is

$$\sum_{0\leqslant k<m}\left\lfloor\frac{nk+x}{m}\right\rfloor = d\left\lfloor\frac{x}{d}\right\rfloor + \frac{m-1}{2}n + \frac{d-m}{2},$$

where $d=\gcd(m,n)$. As a check, we can make sure this works in the special cases $n=0$ and $n=1$ that we knew before: When $n=0$ we get $d=\gcd(m,0)=m$; the last two terms of the formula are zero so the formula properly gives $m\lfloor x/m\rfloor$. And for $n=1$ we get $d=\gcd(m,1)=1$; the last two terms cancel nicely, and the sum is just $\lfloor x\rfloor$.

By manipulating the closed form a bit, we can actually make it symmetric in m and n:

$$\begin{aligned}\sum_{0\leqslant k<m}\left\lfloor\frac{nk+x}{m}\right\rfloor &= d\left\lfloor\frac{x}{d}\right\rfloor + \frac{m-1}{2}n + \frac{d-m}{2}\\ &= d\left\lfloor\frac{x}{d}\right\rfloor + \frac{(m-1)(n-1)}{2} + \frac{m-1}{2} + \frac{d-m}{2}\\ &= d\left\lfloor\frac{x}{d}\right\rfloor + \frac{(m-1)(n-1)}{2} + \frac{d-1}{2}. \end{aligned} \qquad (3.32)$$

This is astonishing, because there's no algebraic reason to suspect that such a sum should be symmetrical. We have proved a "reciprocity law,"

Yup, I'm floored.

$$\sum_{0\leqslant k<m}\left\lfloor\frac{nk+x}{m}\right\rfloor = \sum_{0\leqslant k<n}\left\lfloor\frac{mk+x}{n}\right\rfloor, \qquad \text{integers } m,n>0.$$

For example, if $m=41$ and $n=127$, the left sum has 41 terms and the right has 127; but they still come out equal, for all real x.

Exercises

Warmups

1 When we analyzed the Josephus problem in Chapter 1, we represented an arbitrary positive integer n in the form $n = 2^m + l$, where $0 \leqslant l < 2^m$. Give explicit formulas for l and m as functions of n, using floor and/or ceiling brackets.

2 What is a formula for the nearest integer to a given real number x? In case of ties, when x is exactly halfway between two integers, give an expression that rounds (a) up — that is, to $\lceil x \rceil$; (b) down — that is, to $\lfloor x \rfloor$.

3 Evaluate $\lfloor \lfloor m\alpha \rfloor n/\alpha \rfloor$, when m and n are positive integers and α is an irrational number greater than n.

4 The text describes problems at levels 1 through 5. What is a level 0 problem? (This, by the way, is *not* a level 0 problem.)

5 Find a necessary and sufficient condition that $\lfloor nx \rfloor = n\lfloor x \rfloor$, when n is a positive integer. (Your condition should involve $\{x\}$.)

6 Can something interesting be said about $\lfloor f(x) \rfloor$ when $f(x)$ is a continuous, monotonically *decreasing* function that takes integer values only when x is an integer?

7 Solve the recurrence

$$\begin{aligned} X_n &= n\,, && \text{for } 0 \leqslant n < m; \\ X_n &= X_{n-m} + 1\,, && \text{for } n \geqslant m. \end{aligned}$$

You know you're in college when the book doesn't tell you how to pronounce 'Dirichlet'.

8 Prove the *Dirichlet box principle*: If n objects are put into m boxes, some box must contain $\geqslant \lceil n/m \rceil$ objects, and some box must contain $\leqslant \lfloor n/m \rfloor$.

9 Egyptian mathematicians in 1800 B.C. represented rational numbers between 0 and 1 as sums of unit fractions $1/x_1 + \cdots + 1/x_k$, where the x's were distinct positive integers. For example, they wrote $\frac{1}{3} + \frac{1}{15}$ instead of $\frac{2}{5}$. Prove that it is always possible to do this in a systematic way: If $0 < m/n < 1$, then

$$\frac{m}{n} = \frac{1}{q} + \left\{\text{representation of } \frac{m}{n} - \frac{1}{q}\right\}, \qquad q = \left\lceil \frac{n}{m} \right\rceil.$$

(This is *Fibonacci's algorithm*, due to Leonardo Fibonacci, A.D. 1202.)

Basics

10 Show that the expression

$$\left\lceil \frac{2x+1}{2} \right\rceil - \left\lceil \frac{2x+1}{4} \right\rceil + \left\lfloor \frac{2x+1}{4} \right\rfloor$$

is always either $\lfloor x \rfloor$ or $\lceil x \rceil$. In what circumstances does each case arise?

11 Give details of the proof alluded to in the text, that the open interval $(\alpha\,..\,\beta)$ contains exactly $\lceil \beta \rceil - \lfloor \alpha \rfloor - 1$ integers when $\alpha < \beta$. Why does the case $\alpha = \beta$ have to be excluded in order to make the proof correct?

12 Prove that

$$\left\lceil \frac{n}{m} \right\rceil = \left\lfloor \frac{n+m-1}{m} \right\rfloor ,$$

for all integers n and all positive integers m. [This identity gives us another way to convert ceilings to floors and vice versa, instead of using the reflective law (3.4).]

13 Let α and β be positive real numbers. Prove that $\mathrm{Spec}(\alpha)$ and $\mathrm{Spec}(\beta)$ partition the positive integers if and only if α and β are irrational and $1/\alpha + 1/\beta = 1$.

14 Prove or disprove:

$$(x \bmod ny) \bmod y = x \bmod y\,, \qquad \text{integer } n.$$

15 Is there an identity analogous to (3.26) that uses ceilings instead of floors?

16 Prove that $n \bmod 2 = \bigl(1-(-1)^n\bigr)/2$. Find and prove a similar expression for $n \bmod 3$ in the form $a+b\omega^n+c\omega^{2n}$, where ω is the complex number $(-1+i\sqrt{3}\,)/2$. *Hint:* $\omega^3 = 1$ and $1+\omega+\omega^2 = 0$.

17 Evaluate the sum $\sum_{0 \leqslant k < m} \lfloor x + k/m \rfloor$ in the case $x \geqslant 0$ by substituting $\sum_j [1 \leqslant j \leqslant x + k/m]$ for $\lfloor x + k/m \rfloor$ and summing first on k. Does your answer agree with (3.26)?

18 Prove that the boundary-value error term S in (3.30) is at most $\lceil \alpha^{-1} v \rceil$. *Hint:* Show that small values of j are not involved.

Homework exercises

19 Find a necessary and sufficient condition on the real number $b > 1$ such that

$$\lfloor \log_b x \rfloor = \bigl\lfloor \log_b \lfloor x \rfloor \bigr\rfloor$$

for all real $x \geqslant 1$.

20 Find the sum of all multiples of x in the closed interval $[\alpha \mathinner{.\,.} \beta]$, when $x > 0$.

21 How many of the numbers 2^m, for $0 \leqslant m \leqslant M$, have leading digit 1 in decimal notation?

22 Evaluate the sums $S_n = \sum_{k \geqslant 1} \lfloor n/2^k + \frac{1}{2} \rfloor$ and $T_n = \sum_{k \geqslant 1} 2^k \lfloor n/2^k + \frac{1}{2} \rfloor^2$.

23 Show that the nth element of the sequence

$$1, 2, 2, 3, 3, 3, 4, 4, 4, 4, 5, 5, 5, 5, 5, \ldots$$

is $\lfloor \sqrt{2n} + \frac{1}{2} \rfloor$. (The sequence contains exactly m occurrences of m.)

24 Exercise 13 establishes an interesting relation between the two multisets $\mathrm{Spec}(\alpha)$ and $\mathrm{Spec}\bigl(\alpha/(\alpha-1)\bigr)$, when α is any irrational number > 1, because $1/\alpha + (\alpha-1)/\alpha = 1$. Find (and prove) an interesting relation between the two multisets $\mathrm{Spec}(\alpha)$ and $\mathrm{Spec}\bigl(\alpha/(\alpha+1)\bigr)$, when α is any positive real number.

25 Prove or disprove that the Knuth numbers, defined by (3.16), satisfy $K_n \geqslant n$ for all nonnegative n.

26 Show that the auxiliary Josephus numbers (3.20) satisfy

$$\left(\frac{q}{q-1}\right)^n \leqslant D_n^{(q)} \leqslant q\left(\frac{q}{q-1}\right)^n, \qquad \text{for } n \geqslant 0.$$

27 Prove that infinitely many of the numbers $D_n^{(3)}$ defined by (3.20) are even, and that infinitely many are odd.

28 Solve the recurrence

$$\begin{aligned} a_0 &= 1; \\ a_n &= a_{n-1} + \lfloor \sqrt{a_{n-1}} \rfloor, \qquad \text{for } n > 0. \end{aligned}$$

There's a discrepancy between this formula and (3.31).

29 Show that, in addition to (3.31), we have

$$D(\alpha, n) \geqslant D(\alpha', \lfloor \alpha n \rfloor) - \alpha^{-1} - 2.$$

30 Show that the recurrence

$$\begin{aligned} X_0 &= m, \\ X_n &= X_{n-1}^2 - 2, \qquad \text{for } n > 0, \end{aligned}$$

has the solution $X_n = \lceil \alpha^{2^n} \rceil$, if m is an integer greater than 2, where $\alpha + \alpha^{-1} = m$ and $\alpha > 1$. For example, if $m = 3$ the solution is

$$X_n = \lceil \phi^{2^{n+1}} \rceil, \qquad \phi = \frac{1+\sqrt{5}}{2}, \qquad \alpha = \phi^2.$$

31 Prove or disprove: $\lfloor x \rfloor + \lfloor y \rfloor + \lfloor x+y \rfloor \leqslant \lfloor 2x \rfloor + \lfloor 2y \rfloor$.

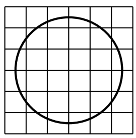
32 Let $\|x\| = \min\bigl(x - \lfloor x \rfloor, \lceil x \rceil - x\bigr)$ denote the distance from x to the nearest integer. What is the value of

$$\sum_k 2^k \|x/2^k\|^2 \,?$$

(Note that this sum can be doubly infinite. For example, when $x = 1/3$ the terms are nonzero as $k \to -\infty$ and also as $k \to +\infty$.)

Exam problems

33 A circle, $2n-1$ units in diameter, has been drawn symmetrically on a $2n \times 2n$ chessboard, illustrated here for $n = 3$:



a How many cells of the board contain a segment of the circle?

b Find a function $f(n,k)$ such that exactly $\sum_{k=1}^{n-1} f(n,k)$ cells of the board lie entirely within the circle.

34 Let $f(n) = \sum_{k=1}^{n} \lceil \lg k \rceil$.

a Find a closed form for $f(n)$, when $n \geqslant 1$.

b Prove that $f(n) = n - 1 + f\bigl(\lceil n/2 \rceil\bigr) + f\bigl(\lfloor n/2 \rfloor\bigr)$ for all $n \geqslant 1$.

35 Simplify the formula $\bigl\lfloor (n+1)^2 n!\, e \bigr\rfloor \bmod n$.

Simplify it, but don't change the value.

36 Assuming that n is a nonnegative integer, find a closed form for the sum

$$\sum_{1 < k < 2^{2^n}} \frac{1}{2^{\lfloor \lg k \rfloor} 4^{\lfloor \lg \lg k \rfloor}} \,.$$

37 Prove the identity

$$\sum_{0 \leqslant k < m} \left(\left\lfloor \frac{m+k}{n} \right\rfloor - \left\lfloor \frac{k}{n} \right\rfloor \right) = \left\lfloor \frac{m^2}{n} \right\rfloor - \left\lfloor \frac{\min\bigl(m \bmod n, (-m) \bmod n\bigr)^2}{n} \right\rfloor$$

for all positive integers m and n.

38 Let $x_1, \ldots, x_n$ be real numbers such that the identity

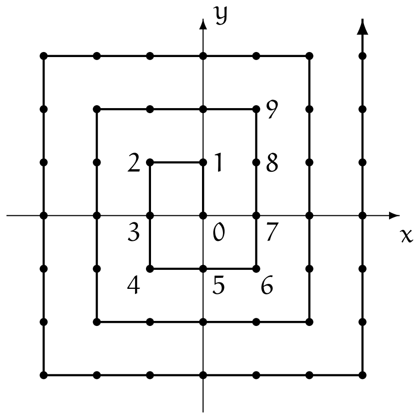
$$\sum_{k=1}^{n} \lfloor m x_k \rfloor = \left\lfloor m \sum_{1 \leqslant k \leqslant n} x_k \right\rfloor$$

holds for all positive integers m. Prove something interesting about $x_1, \ldots, x_n$.

People in the southern hemisphere use a different spiral.

39 Prove that the double sum $\sum_{0\leqslant k\leqslant \log_b x}\sum_{0<j<b}\lceil (x+jb^k)/b^{k+1}\rceil$ equals $(b-1)\big(\lfloor \log_b x\rfloor + 1\big) + \lceil x\rceil - 1$, for every real number $x \geqslant 1$ and every integer $b > 1$.

40 The spiral function $\sigma(n)$, indicated in the diagram below, maps a nonnegative integer n onto an ordered pair of integers $\big(x(n), y(n)\big)$. For example, it maps $n = 9$ onto the ordered pair $(1, 2)$.



a Prove that if $m = \lfloor \sqrt{n}\rfloor$,

$$x(n) \;=\; (-1)^m\Big(\big(n - m(m+1)\big)\cdot\big[\lfloor 2\sqrt{n}\rfloor \text{ is even}\big] + \lceil \tfrac{1}{2}m\rceil\Big)\,,$$

and find a similar formula for $y(n)$. *Hint:* Classify the spiral into segments W_k, S_k, E_k, N_k according as $\lfloor 2\sqrt{n}\rfloor = 4k-2$, $4k-1$, $4k$, $4k+1$.

b Prove that, conversely, we can determine n from $\sigma(n)$ by a formula of the form

$$n \;=\; (2k)^2 \pm \big(2k + x(n) + y(n)\big)\,, \quad k \;=\; \max\big(|x(n)|, |y(n)|\big).$$

Give a rule for when the sign is $+$ and when the sign is $-$.

Bonus problems

41 Let f and g be increasing functions such that the sets $\{f(1), f(2), \ldots\}$ and $\{g(1), g(2), \ldots\}$ partition the positive integers. Suppose that f and g are related by the condition $g(n) = f\big(f(n)\big) + 1$ for all $n > 0$. Prove that $f(n) = \lfloor n\phi\rfloor$ and $g(n) = \lfloor n\phi^2\rfloor$, where $\phi = (1+\sqrt{5}\,)/2$.

42 Do there exist real numbers α, β, and γ such that Spec(α), Spec(β), and Spec(γ) together partition the set of positive integers?

43 Find an interesting interpretation of the Knuth numbers, by unfolding the recurrence (3.16).

44 Show that there are integers $a_n^{(q)}$ and $d_n^{(q)}$ such that

$$a_n^{(q)} = \frac{D_{n-1}^{(q)} + d_n^{(q)}}{q-1} = \frac{D_n^{(q)} + d_n^{(q)}}{q}, \qquad \text{for } n > 0,$$

when $D_n^{(q)}$ is the solution to (3.20). Use this fact to obtain another form of the solution to the generalized Josephus problem:

$$J_q(n) = 1 + d_k^{(q)} + q(n - a_k^{(q)}), \qquad \text{for } a_k^{(q)} \leqslant n < a_{k+1}^{(q)}.$$

45 Extend the trick of exercise 30 to find a closed-form solution to

$$Y_0 = m,$$
$$Y_n = 2Y_{n-1}^2 - 1, \qquad \text{for } n > 0,$$

if m is a positive integer.

46 Prove that if $n = \lfloor(\sqrt{2}^{\,l} + \sqrt{2}^{\,l-1})m\rfloor$, where m and l are nonnegative integers, then $\lfloor\sqrt{2n(n+1)}\rfloor = \lfloor(\sqrt{2}^{\,l+1} + \sqrt{2}^{\,l})m\rfloor$. Use this remarkable property to find a closed form solution to the recurrence

$$L_0 = a, \qquad \text{integer } a > 0;$$
$$L_n = \lfloor\sqrt{2L_{n-1}(L_{n-1}+1)}\rfloor, \qquad \text{for } n > 0.$$

Hint: $\lfloor\sqrt{2n(n+1)}\rfloor = \lfloor\sqrt{2}(n+\frac{1}{2})\rfloor$.

47 The function $f(x)$ is said to be *replicative* if it satisfies

$$f(mx) = f(x) + f\Big(x + \frac{1}{m}\Big) + \cdots + f\Big(x + \frac{m-1}{m}\Big)$$

for every positive integer m. Find necessary and sufficient conditions on the real number c for the following functions to be replicative:

a $f(x) = x + c$.

b $f(x) = [x + c \text{ is an integer}]$.

c $f(x) = \max(\lfloor x\rfloor, c)$.

d $f(x) = x + c\lfloor x\rfloor - \frac{1}{2}[x \text{ is not an integer}]$.

48 Prove the identity

$$x^3 = 3x\lfloor x\lfloor x\rfloor\rfloor + 3\{x\}\{x\lfloor x\rfloor\} + \{x\}^3 - 3\lfloor x\rfloor\lfloor x\lfloor x\rfloor\rfloor + \lfloor x\rfloor^3,$$

and show how to obtain similar formulas for x^n when $n > 3$.

49 Find a necessary and sufficient condition on the real numbers $0 \leqslant \alpha < 1$ and $\beta \geqslant 0$ such that we can determine α and β from the infinite multiset of values

$$\big\{ \lfloor n\alpha \rfloor + \lfloor n\beta \rfloor \;\big|\; n > 0 \big\} .$$

Research problems

50 Find a necessary and sufficient condition on the nonnegative real numbers α and β such that we can determine α and β from the infinite multiset of values

$$\big\{ \big\lfloor \lfloor n\alpha \rfloor \beta \big\rfloor \;\big|\; n > 0 \big\} .$$

51 Let x be a real number $\geqslant \phi = \frac{1}{2}(1+\sqrt{5})$. The solution to the recurrence

$$\begin{aligned} Z_0(x) &= x\,, \\ Z_n(x) &= Z_{n-1}(x)^2 - 1\,, \qquad \text{for } n > 0, \end{aligned}$$

can be written $Z_n(x) = \big\lceil f(x)^{2^n} \big\rceil$, if x is an integer, where

$$f(x) \;=\; \lim_{n\to\infty} Z_n(x)^{1/2^n} ,$$

because $Z_n(x)-1 < f(x)^{2^n} < Z_n(x)$ in that case. What other interesting properties does this function $f(x)$ have?

52 Given nonnegative real numbers α and β, let

$$\operatorname{Spec}(\alpha;\beta) \;=\; \big\{ \lfloor \alpha+\beta \rfloor, \lfloor 2\alpha+\beta \rfloor, \lfloor 3\alpha+\beta \rfloor, \ldots \big\}$$

Spec this be hard.

be a multiset that generalizes $\operatorname{Spec}(\alpha) = \operatorname{Spec}(\alpha;0)$. Prove or disprove: If the $m \geqslant 3$ multisets $\operatorname{Spec}(\alpha_1;\beta_1)$, $\operatorname{Spec}(\alpha_2;\beta_2)$, $\ldots$, $\operatorname{Spec}(\alpha_m;\beta_m)$ partition the positive integers, and if the parameters $\alpha_1 < \alpha_2 < \cdots < \alpha_m$ are rational, then

$$\alpha_k \;=\; \frac{2^m-1}{2^{k-1}} , \qquad \text{for } 1 \leqslant k \leqslant m.$$

53 Fibonacci's algorithm (exercise 9) is "greedy" in the sense that it chooses the least conceivable q at every step. A more complicated algorithm is known by which every fraction m/n with n odd can be represented as a sum of distinct unit fractions $1/q_1 + \cdots + 1/q_k$ with *odd* denominators. Does the greedy algorithm for such a representation always terminate?

Index

(Graffiti have been indexed too.)

WHEN AN INDEX ENTRY refers to a page containing a relevant exercise, the answer to that exercise (in Appendix A) might divulge further information; an answer page is not indexed here unless it refers to a topic that isn't included in the statement of the relevant exercise. Some notations not indexed here (like $x^{\underline{n}}$, $\lfloor x \rfloor$, and $\left\langle {n \atop m} \right\rangle$) are listed on pages x and xi, just before the table of contents.

List of Tables

THIS BOOK was composed at Stanford University using the TEX system for technical text developed by D. E. Knuth. The mathematics is set in a new typeface called AMS Euler (Version 2.1), designed by Hermann Zapf for the American Mathematical Society. The text is set in a new typeface called Concrete Roman and Italic, a special version of Knuth's Computer Modern family with weights designed to blend with AMS Euler. The paper is 50-lb.-basis Bright White Finch Opaque, which has a neutral pH and a life expectancy of several hundred years. The offset printing and notch binding were done by the Courier Corporation of Westford, Massachusetts.

This book introduces the mathematics that supports advanced computer programming and the analysis of algorithms. The primary aim of its well-known authors is to provide a solid and relevant base of mathematical skills — the skills needed to solve complex problems, to evaluate horrendous sums, and to discover subtle patterns in data. It is an indispensable text and reference not only for computer scientists — the authors themselves rely heavily on it! — but for serious users of mathematics in virtually every discipline.

Concrete mathematics is a blending of CONtinuous and disCRETE mathematics. "More concretely," the authors explain, "it is the controlled manipulation of mathematical formulas, using a collection of techniques for solving problems." The subject matter is primarily an expansion of the Mathematical Preliminaries section in Knuth's classic *Art of Computer Programming*, but the style of presentation is more leisurely, and individual topics are covered more deeply. Several new topics have been added, and the most significant ideas have been traced to their historical roots. The book includes more than 500 exercises, divided into six categories. Complete answers are provided for all exercises, except research problems, making the book particularly valuable for self-study.

Major topics include:

Sums • Recurrences • Integer functions • Elementary number theory • Binomial coefficients • Generating functions • Discrete probability • Asymptotic methods

This second edition includes important new material about mechanical summation. In response to the widespread use of the first edition as a reference book, the bibliography and index have also been expanded, and additional nontrivial improvements can be found on almost every page.

Readers will appreciate the informal style of *Concrete Mathematics*. Particularly enjoyable are the marginal graffiti contributed by students who have taken courses based on this material. Graham, Knuth, and Patashnik want to convey not only the importance of the techniques presented, but some of the fun in learning and using them.

About the authors:

RONALD L. GRAHAM is Chief Scientist at AT&T Labs Research. He is also University Professor of Mathematical Sciences at Rutgers University, and a former President of the American Mathematical Society. Dr. Graham is the author of six other mathematics books.

DONALD E. KNUTH is Professor Emeritus of The Art of Computer Programming at Stanford University. His prolific writings include three volumes on the *Art of Computer Programming*, and five books related to his TEX and METAFONT typesetting systems.

OREN PATASHNIK is a member of the research staff at the Center for Communications Research, La Jolla. He is also the author of BibTEX, a widely used bibliography processor.