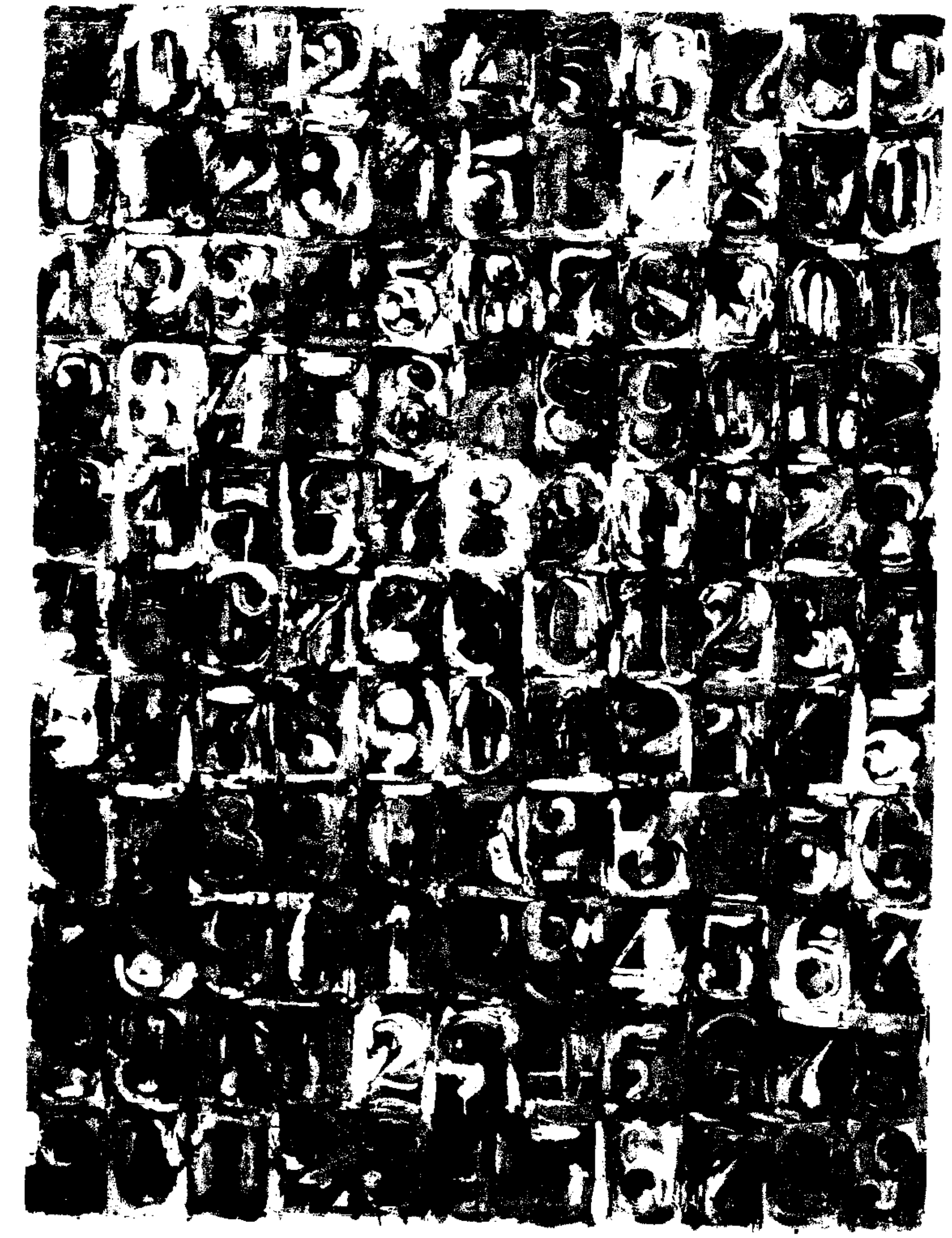
THE MAGIC OF NUMBERS



Benedict Gross • Joe Harris

CONTENTS

Preface xiii

PART I COUNTING 1

Chapter 1

Simple Counting 3

1.1 Counting Numbers 3
1.2 Counting Divisible Numbers 5
1.3 "I've reduced it to a previously solved problem" 6
1.4 Really Big Numbers 7
1.5 It Could Be Worse 8

Chapter 2

The Multiplication Principle 11

2.1 Choices 11
2.2 More Examples 12
2.3 Two Formulas 15
2.4 Factorials 16
2.5 Another Wrinkle 18

Chapter 3

The Subtraction Principle 20

3.1 Back to the Video Store 20
3.2 Some More Problems 22
3.3 Multiple Subtractions 25

Chapter 4

Collections 28

4.1 Back to the House of Pizza 28
4.2 Binomial Coefficients 29
4.3 Examples 34
4.4 Multinomials 40
4.5 Something's Missing 43

CONTENTS

Preface xiii

PART I COUNTING 1

Chapter 1

Simple Counting 3

- 1.1 Counting Numbers 3
- 1.2 Counting Divisible Numbers 5
- 1.3 "I've reduced it to a previously solved problem" 6
- 1.4 Really Big Numbers 7
- 1.5 It Could Be Worse 8

Chapter 2

The Multiplication Principle 11

- 2.1 Choices 11
- 2.2 More Examples 12
- 2.3 Two Formulas 15
- 2.4 Factorials 16
- 2.5 Another Wrinkle 18

Chapter 3

The Subtraction Principle 20

- 3.1 Back to the Video Store 20
- 3.2 Some More Problems 22
- 3.3 Multiple Subtractions 25

Chapter 4

Collections 28

- 4.1 Back to the House of Pizza 28
- 4.2 Binomial Coefficients 29
- 4.3 Examples 34
- 4.4 Multinomials 40
- 4.5 Something's Missing 43

Chapter 5
Probability 46

5.1 Flipping Coins 46
5.2 Tumbling Dice 48
5.3 Playing Poker 51
5.4 Really Playing Poker 55
5.5 Bridge 56
5.6 The Birthday Problem 58

Chapter 6
Pascal's Triangle and the Binomial Theorem 59

6.1 Pascal's Triangle 59
6.2 A New Relation 60
6.3 More Relations 63
6.4 The Binomial Theorem 66

Chapter 7
Advanced Counting 69

7.1 Back to the Fruit Bowl 69
7.2 Catalan Numbers 74
7.3 A Recursion Relation 75
7.4 Another Interpretation 77
7.5 The Closed Formula 79
7.6 The Derivation 79
7.7 Why Do We Do These Things, Anyway? 84

PART II ARITHMETIC 87

Chapter 8
Divisibility 89

8.1 What Numbers *Are* Divisible by Both 4 and 6? 89
8.2 Least Common Multiples 91
8.3 Greatest Common Divisors 93
8.4 Euclid's Algorithm 94
8.5 Who Was Euclid? What's an Algorithm? 97

Chapter 9
Combinations 99
9.1 Pixels, Grackls, and Pancakes 99
9.2 Combinations 100
9.3 Finding Explicit Solutions 103
9.4 Any More Questions? 105

Chapter 10
Primes 109
10.1 What Is a Prime? 109
10.2 Prime Factorization 110
10.3 The Sieve of Eratosthenes 111
10.4 Some Questions 113
10.5 How Many Primes Are There? 114
10.6 Prime Deserts and Twin Primes 115

Chapter 11
Factorization 117
11.1 A Note About the Exercises 117
11.2 What a Prime Is, Really 118
11.3 Binomial Coefficients Again 121
11.4 The Fundamental Theorem of Arithmetic 122
11.5 It's a Matter of Chemistry 123

Chapter 12
Consequences 126
12.1 Preliminaries 126
12.2 Multiplication and Division 127
12.3 How Many Numbers Divide 756? 129
12.4 gcd's and lcm's 130
12.5 Factorials Again 132
12.6 $\sqrt{2}$ Is Not a Fraction 133
12.7 The Fine Print 135

Chapter 13
Relatively Prime 138
13.1 What Does It Mean to Be Relatively Prime? 138
13.2 The Euler ϕ-function 140
13.3 Why Does this Work? 143
13.4 Odds and Ends 145

Chapter 5

Probability 46

5.1 Flipping Coins 46
5.2 Tumbling Dice 48
5.3 Playing Poker 51
5.4 Really Playing Poker 55
5.5 Bridge 56
5.6 The Birthday Problem 58

Chapter 6

Pascal's Triangle and the Binomial Theorem 59

6.1 Pascal's Triangle 59
6.2 A New Relation 60
6.3 More Relations 63
6.4 The Binomial Theorem 66

Chapter 7

Advanced Counting 69

7.1 Back to the Fruit Bowl 69
7.2 Catalan Numbers 74
7.3 A Recursion Relation 75
7.4 Another Interpretation 77
7.5 The Closed Formula 79
7.6 The Derivation 79
7.7 Why Do We Do These Things, Anyway? 84

PART II ARITHMETIC 87

Chapter 8

Divisibility 89

8.1 What Numbers *Are* Divisible by Both 4 and 6? 89
8.2 Least Common Multiples 91
8.3 Greatest Common Divisors 93
8.4 Euclid's Algorithm 94
8.5 Who Was Euclid? What's an Algorithm? 97

Chapter 9

Combinations 99

9.1 Pixels, Grackls, and Pancakes 99
9.2 Combinations 100
9.3 Finding Explicit Solutions 103
9.4 Any More Questions? 105

Chapter 10

Primes 109

10.1 What Is a Prime? 109
10.2 Prime Factorization 110
10.3 The Sieve of Eratosthenes 111
10.4 Some Questions 113
10.5 How Many Primes Are There? 114
10.6 Prime Deserts and Twin Primes 115

Chapter 11

Factorization 117

11.1 A Note About the Exercises 117
11.2 What a Prime Is, Really 118
11.3 Binomial Coefficients Again 121
11.4 The Fundamental Theorem of Arithmetic 122
11.5 It's a Matter of Chemistry 123

Chapter 12

Consequences 126

12.1 Preliminaries 126
12.2 Multiplication and Division 127
12.3 How Many Numbers Divide 756? 129
12.4 gcd's and lcm's 130
12.5 Factorials Again 132
12.6 $\sqrt{2}$ Is Not a Fraction 133
12.7 The Fine Print 135

Chapter 13

Relatively Prime 138

13.1 What Does It Mean to Be Relatively Prime? 138
13.2 The Euler ϕ-function 140
13.3 Why Does this Work? 143
13.4 Odds and Ends 145

Chapter 23

Finding Primes 260

23.1 How Frequently Do Primes Occur? 260
23.2 Many, Many Questions 262
23.3 How Primes Are Found 263
23.4 Mathematicians and Logic 264
23.5 Is 21 a Prime? 265
23.6 Can I Get a Witness 265
23.7 It's Always Something 266
23.8 How Many Square Roots of 1 Are There in Modular Arithmetic? 268
23.9 The Miller-Rabin Test 269

Chapter 24

Generators, Roots, and Passwords 272

24.1 Generators 273
24.2 More on Square Roots 275
24.3 Square Roots of -1 276
24.4 Congruence Classes of Primes 279
24.5 Counting Generators 280
24.6 "Swordfish" 281
24.7 Time to Say Goodbye 282

Index 285

PREFACE

The primarily purpose of the preface to a textbook is to convey a sense of the goals of the book, and to a lesser extent its level, pace and language. Since this book is based on a course, Quantitative Reasoning 28, that we developed at Harvard University, it seems reasonable to start by describing the goals of that course.

There are, it seems to us, two strains in our educational system, reflecting two disparate aims. One is preprofessional: among the courses you take in high school and in college are those that will, it's hoped, provide you with the basis of the discipline that will become your vocation in later life. The other strain, by contrast, seeks to enrich your life: to expose you to ideas and modes of thought that you might not come in contact with otherwise. This is one of the ideas underlying Harvard's Core Program, and QR28 was developed as a Core course. It's not a technical course, designed to prepare you for the next course; rather, it's simply a collection of topics that we find fascinating, and that make up a coherent whole. Our hope is that we will be able to communicate to you some idea of the mathematical view of the world, and of what attracts people to math in the first place.

Probably the best way to describe the course is by analogy: you might think of it as a math appreciation course, to be taken in the same spirit as you would a music appreciation course. We're not trying to teach you how to write a symphony, or to play the violin; we simply want you to be able to hear the music.

Or you might think of it like an introductory language course—say, Italian—that you take for fun and because it's such a beautiful language. This analogy is particularly apt in one respect. The heart of a language course is not the memorization of a lot of vocabulary and verb tenses—though there's inevitably a lot of that involved—but rather the experience of thinking and speaking in a different tongue. In the same way, in this text there are of necessity a fair number of techniques to learn and calculations to carry out, but that's just the means to an end: our goal, ultimately, is to give you the experience of thinking in math.

What sort of prerequisites does this book have? Well, the technical answer to that is "virtually none": junior high school algebra will cover it handily. (To be concrete, if you can add fractions, and are reasonably comfortable with the use of letters to stand for numbers, you should be solid.) Probably more important, though, is a less quantifiable requirement: we would ask that the reader be prepared to approach the book in a spirit of adventure and exploration, and with the understanding that, while some work will be required, the experience will be worth it.

Additional exercises, problems, and sample exams are available at www.prenhall.com/gross.

Acknowledgments

We are indebted to a great number of people for help in creating this book. Susan Milano gave us the name for the course and, by extension, the book, and also read and critiqued an early version. Sarah Brelsfoard and Debby Green also did a

wonderful job of reading the first draft and pointing out mistakes. We owe a debt to Ivan Niven and his book, *Mathematics of Choice*, which has clearly influenced our treatment of the topics in the first part of this book. We would also like to thank the reviewers, Robert Bernhardt of East Carolina University, Fernando Gouvêa of Colby College, Steven Krantz of Washington University, and M. Terrell of Cornell University, for many helpful comments and corrections. And our editors, particularly Erin Mulligan, Bayani Mendoza de Leon, Petra Recter, and Sally Yagan, have been terrifically helpful, as has our compositor at Laserwords.

Inasmuch as this book represents a print version of the course QR28, it could not exist without the help of all those who made the course what it is. Susan Lewis, the director of the Core Program at Harvard, first encouraged us to develop a course in mathematics for this program. Then there are all the people who helped shape the course: our Head Teaching Fellows Tom Weston, Rob Pollack, Elena Mantovan and Nick Rogers; our other Teaching Fellows Sam Williams, Tomas Klenke, Stephanie Yang, Laura DeMarco, Mark Lucianovic, Sarah Dean, Robert Neel and Marty Weissman. And, of course, all the students who took the course from 1999 through 2002.

Benedict Gross

Joe Harris

PART I

Counting