

TURING

图灵原版数学·统计学系列 38

CAMBRIDGE

Combinatorics

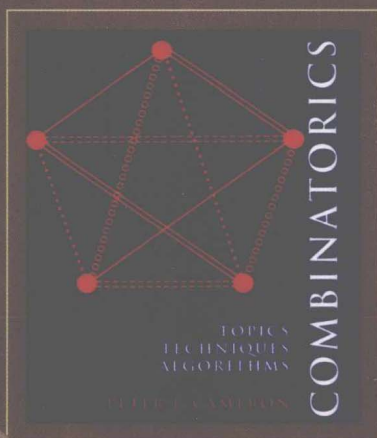
Topics, Techniques, Algorithms

组合数学

专题、技术与算法

(英文版)

[英] Peter J. Cameron 著



人民邮电出版社
POSTS & TELECOM PRESS



图灵原版数学·统计学系列

Combinatorics

Topics, Techniques, Algorithms

组合数学

[英] Peter J. Cameron 著

人民邮电出版社
北 京

图书在版编目 (CIP) 数据

组合数学: 专题、技术与算法 = Combinatorics: Topics, Techniques, Algorithms; 英文/ (英) 卡梅伦 (Cameron, P. J.) 著. —北京: 人民邮电出版社, 2009.8
(图灵原版数学·统计学系列)
ISBN 978-7-115-21087-6

I. 组… II. 卡… III. 组合数学—英文 IV. O157

中国版本图书馆CIP数据核字 (2009) 第100513号

内 容 提 要

这本优秀的组合数学教材是作者20多年研究和教学经验的结晶。全书分成初级篇和高级篇两个部分, 共18章内容, 每章都以“专题—技术—算法”的模式呈现, 阐述深入浅出, 简明易懂。本书几乎涵盖了组合数学中所有有趣的主题, 如中国邮递员问题、中国的九连环问题、友谊定理等, 当然也收集了若干前沿内容。

本书适合作为高等院校高年级本科生与低年级研究生的组合数学课程教材, 也适合各理工学科科研人员参考。

图灵原版数学·统计学系列

组合数学: 专题、技术与算法(英文版)

-
- ◆ 著 [英] Peter J. Cameron
责任编辑 明永玲
- ◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街14号
邮编 100061 电子函件 315@ptpress.com.cn
网址 <http://www.ptpress.com.cn>
北京隆昌伟业印刷有限公司印刷
- ◆ 开本: 700×1000 1/16
印张: 22.75
字数: 362千字 2009年8月第1版
印数: 1-2 000册 2009年8月北京第1次印刷
著作权合同登记号 图字: 01-2009-2917号
ISBN 978-7-115-21087-6/O1
-

定价: 59.00元

读者服务热线: (010) 51095186 印装质量热线: (010) 67129223

反盗版热线: (010) 67171154

版 权 声 明

Combinatorics: Topics, Techniques, Algorithms (978-0-521-45761-3) by Peter J. Cameron first published by Cambridge University Press 1994.

All rights reserved.

This reprint edition for the People's Republic of China is published by arrangement with the Press Syndicate of the University of Cambridge, Cambridge, United Kingdom.

© Cambridge University Press & POSTS & TELECOM PRESS 2009.

This book is in copyright. No reproduction of any part may take place without the written permission of Cambridge University Press and POSTS & TELECOM PRESS.

This edition is for sale in the People's Republic of China (excluding Hong Kong SAR, Macao SAR and Taiwan Province) only.

此版本仅限在中华人民共和国境内（不包括香港、澳门特别行政区及台湾地区）销售。

Preface

I've got to work the E quations and the low cations
I've got to comb the nations of it.

Russell Hoban, *Riddley Walker* (1980)

We have not begun to understand the relationship between combinatorics and
conceptual mathematics.

J. Dieudonné, *A Panorama of Pure Mathematics* (1982)

If anything at all can be deduced from the two quotations at the top of this page, perhaps it is this: Combinatorics is an essential part of the human spirit; but it is a difficult subject for the abstract, axiomatising Bourbaki school of mathematics to comprehend. Nevertheless, the advent of computers and electronic communications have made it a more important subject than ever.

This is a textbook on combinatorics. It's based on my experience of more than twenty years of research and, more specifically, on teaching a course at Queen Mary and Westfield College, University of London, since 1986. The book presupposes some mathematical knowledge. The first part (Chapters 2–11) could be studied by a second-year British undergraduate; but I hope that more advanced students will find something interesting here too (especially in the Projects, which may be skipped without much loss by beginners). The second half (Chapters 12–20) is in a more condensed style, more suited to postgraduate students.

I am grateful to many colleagues, friends and students for all kinds of contributions, some of which are acknowledged in the text; and to Neill Cameron, for the illustration on p. 128.

I have not provided a table of dependencies between chapters. Everything is connected; but combinatorics is, by nature, broad rather than deep. The more important connections are indicated at the start of the chapters.

Peter J. Cameron
17 March 1994

Contents

1. What is Combinatorics?	1
<i>Sample problems — How to use this book — What you need to know — Exercises</i>	
2. On numbers and counting	7
<i>Natural numbers and arithmetic — Induction — Some useful functions — Orders of magnitude — Different ways of counting — Double counting — Appendix on set notation — Exercises</i>	
3. Subsets, partitions, permutations	21
<i>Subsets — Subsets of fixed size — The Binomial Theorem and Pascal's Triangle — Project: Congruences of binomial coefficients — Permutations — Estimates for factorials — Selections — Equivalence and order — Project: Finite topologies — Project: Cayley's Theorem on trees — Bell numbers — Generating combinatorial objects — Exercises</i>	
4. Recurrence relations and generating functions	49
<i>Fibonacci numbers — Aside on formal power series — Linear recurrence relations with constant coefficients — Derangements and involutions — Catalan and Bell numbers — Computing solutions to recurrence relations — Project: Finite fields and QUICKSORT — Exercises</i>	
5. The Principle of Inclusion and Exclusion	75
<i>PIE — A generalisation — Stirling numbers — Project: Stirling numbers and exponentials — Even and odd permutations — Exercises</i>	
6. Latin squares and SDRs	87
<i>Latin squares — Systems of distinct representatives — How many Latin squares? — Quasigroups — Project: Quasigroups and groups — Orthogonal Latin squares — Exercises</i>	
7. Extremal set theory	99
<i>Intersecting families — Sperner families — The De Bruijn-Erdős Theorem — Project: Regular families — Exercises</i>	
8. Steiner triple systems	107
<i>Steiner systems — A direct construction — A recursive construction — Packing and covering — Project: Some special Steiner triple systems — Project: Tournaments and Kirkman's schoolgirls — Exercises</i>	
9. Finite geometry	123
<i>Linear algebra over finite fields — Gaussian coefficients — Projective geometry — Axioms for projective geometry — Projective planes — Other kinds of geometry — Project: Coordinates and configurations — Project: Proof of the Bruck-Ryser Theorem — Appendix: Finite fields — Exercises</i>	
10. Ramsey's Theorem	147
<i>The Pigeonhole Principle — Some special cases — Ramsey's Theorem — Bounds for Ramsey numbers — Applications — The infinite version — Exercises</i>	

11. Graphs	159
<i>Definitions — Trees and forests — Minimal spanning trees — Eulerian graphs — Hamiltonian graphs — Project: Gray codes — The Travelling Salesman — Digraphs — Networks — Menger, König and Hall — Diameter and girth — Project: Moore graphs — Exercises</i>	
12. Posets, lattices and matroids	187
<i>Posets and lattices — Linear extensions of a poset — Distributive lattices — Aside on propositional logic — Chains and antichains — Products and dimension — The Möbius function of a poset — Matroids — Project: Arrow's Theorem — Exercises</i>	
13. More on partitions and permutations	209
<i>Partitions, diagrams and conjugacy classes — Euler's Pentagonal Numbers Theorem — Project: Jacobi's Identity — Tableaux — Symmetric polynomials — Exercises</i>	
14. Automorphism groups and permutation groups	225
<i>Three definitions of a group — Examples of groups — Orbits and transitivity — The Schreier-Sims algorithm — Primitivity and multiple transitivity — Examples — Project: Cayley digraphs and Frucht's Theorem — Exercises</i>	
15. Enumeration under group action	245
<i>The Orbit-counting Lemma — An application — Cycle index — Examples — Direct and wreath products — Stirling numbers revisited — Project: Cycle index and symmetric functions — Exercises</i>	
16. Designs	257
<i>Definitions and examples — To repeat or not to repeat — Fisher's Inequality — Designs from finite geometry — Small designs — Project: Hadamard matrices — Exercises</i>	
17. Error-correcting codes	271
<i>Finding out a liar — Definitions — Probabilistic considerations — Some bounds — Linear codes; Hamming codes — Perfect codes — Linear codes and projective spaces — Exercises</i>	
18. Graph colourings	291
<i>More on bipartite graphs — Vertex colourings — Project: Brooks' Theorem — Perfect graphs — Edge colourings — Topological graph theory — Project: The Five-colour Theorem — Exercises</i>	
19. The infinite	307
<i>Counting infinite sets — König's Infinity Lemma — Posets and Zorn's Lemma — Ramsey theory — Systems of distinct representatives — Free constructions — The random graph — Exercises</i>	
20. Where to from here?	325
<i>Computational complexity — Some graph-theoretic topics — Computer software — Unsolved problems — Further reading</i>	
Answers to selected exercises	339
Bibliography	343
Index	347

1. What is Combinatorics?

Combinatorics is the slums of topology.

J. H. C. Whitehead (attr.)¹

I have to admit that he was not bad at combinatorial analysis — a branch, however, that even then I considered to be dried up.

Stanislaw Lem, *His Master's Voice* (1968)

Combinatorics is special. Most mathematical topics which can be covered in a lecture course build towards a single, well-defined goal, such as Cauchy's Theorem or the Prime Number Theorem. Even if such a clear goal doesn't exist, there is a sharp focus (finite groups, perhaps, or non-parametric statistics). By contrast, combinatorics appears to be a collection of unrelated puzzles chosen at random.

Two factors contribute to this. First, combinatorics is broad rather than deep. Its tentacles stretch into virtually all corners of mathematics. Second, it is about techniques rather than results. As in a net,² threads run through the entire construction, appearing unexpectedly far from where we last saw them. A treatment of combinatorics which neglects this is bound to give a superficial impression.

This feature makes the teacher's job harder. Reading, or lecturing, is inherently one-dimensional. If we follow one thread, we miss the essential interconnectedness of the subject.

I have attempted to meet this difficulty by various devices. Each chapter begins with a list of topics, techniques, and algorithms considered in the chapter, and cross-references to other chapters. Also, some of the material is set in smaller type and can be regarded as optional. This usually includes a 'project' involving a more difficult proof or construction (where the arguments may only be sketched, requiring extra work by the reader). These projects could be used for presentations by students. Finally, the book is divided into two parts; the second part treats topics in greater depth, and the pace hots up a bit (though, I hope, not at the expense of intelligibility).

As just noted, there are algorithms scattered throughout the book. These are not computer programs, but descriptions in English of how a computation is performed. I hope that they can be turned into computer programs or subroutines by readers with programming experience. The point is that an explicit construction of an object usually tells us more than a non-constructive existence proof. (Examples will be given to illustrate this.) An algorithm resembles a theorem in that it requires a proof (not of the algorithm itself, but of the fact that it does what is claimed of it).

¹ This attribution is due to Graham Higman, who revised Whitehead's definition to 'Combinatorics is the mews of algebra.'

² 'Net. Anything reticulated or decussated at equal distances, with interstices between the intersections.' Samuel Johnson, *Dictionary of the English Language* (1775).

But what is combinatorics? Why should you read further?

Combinatorics could be described as the art of arranging objects according to specified rules. We want to know, first, whether a particular arrangement is possible at all, and if so, in how many different ways it can be done. If the rules are simple (like picking a cricket team from a class of schoolboys), the existence of an arrangement is clear, and we concentrate on the counting problem. But for more involved rules, it may not be clear whether the arrangement is possible at all. Examples are Kirkman's schoolgirls and Euler's officers, described below.

Sample problems

In this section, I will give four examples of combinatorial questions chosen to illustrate the nature of the subject. Each of these will be discussed later in the book.

Derangements

Given n letters and n addressed envelopes, in how many ways can the letters be placed in the envelopes so that no letter is in the correct envelope?

DISCUSSION. The total number of ways of putting the letters in the envelopes is the number of *permutations* of n objects,³ which is $n!$ (factorial n). We will see that the fraction of these which are all incorrectly addressed is very close to $1/e$, where $e = 2.71828\dots$ is the base of natural logarithms — a surprising result at first sight. In fact, the exact number of ways of mis-addressing all the letters is the nearest integer to $n!/e$ (see Exercise 1).

Kirkman's schoolgirls

Fifteen schoolgirls walk each day in five groups of three. Arrange the girls' walks for a week so that, in that time, each pair of girls walks together in a group just once.

DISCUSSION. If it is possible at all, seven days will be required. For any given girl must walk once with each of the other fourteen; and each day she walks with two others. However, showing that the walks are actually possible requires more argument. The question was posed and solved by Kirkman in 1847. The same question could be asked for other numbers of girls (see Exercise 2). Only in 1967 did Ray-Chaudhuri and Wilson show that solutions exist for any number of girls congruent to 3 modulo 6.

Euler's officers

Thirty-six officers are given, belonging to six regiments and holding six ranks (so that each combination of rank and regiment corresponds to just one officer). Can the officers be paraded in a 6×6 array so that, in any line (row or column) of the array, each regiment and each rank occurs precisely once?

³ Permutations will be described in Chapter 3.

DISCUSSION. Euler posed this problem in 1782; he believed that the answer was 'no'. This was not proved until 1900, by Tarry. Again, the problem can be generalised, to n^2 officers, where the number of regiments, ranks, rows and columns is n (we assume $n > 1$) — see Exercise 3. There is no solution for $n = 2$. Euler knew solutions for all n not congruent to 2 modulo 4, and guessed that there was no solution for $n \equiv 2 \pmod{4}$. However, he was wrong about that. Bose, Shrikhande and Parker showed in 1960 that there is a solution for all n except $n = 2$ and $n = 6$.

A Ramsey game

This two-player game requires a sheet of paper and pencils of two colours, say red and blue. Six points on the paper are chosen, with no three in line. Now the players take a pencil each, and take turns drawing a line connecting two of the chosen points. The first player to complete a triangle of her own colour loses. (Only triangles with vertices at the chosen points count.)

Can the game ever result in a draw?

DISCUSSION. We'll see that a draw is not possible; one or other player will be forced to create a triangle. Ramsey proved a wide generalisation of this fact. His theorem is sometimes stated in the form 'Complete disorder is impossible.'

How to use this book

1. The book is divided into two parts: Chapters 2–11 and Chapters 12–20. In the second part, along with some new material, we revisit many of the topics from the first part and treat them from a more advanced viewpoint; also, as I mentioned earlier, the pace is a little faster in the second part. In any case, a first course can be devised using only the first part of the book. (The second–third year undergraduate course at Queen Mary and Westfield College includes a selection of material from Chapters 3 (Sections 3.1, 3.2, 3.3, 3.5, 3.7, 3.11, 3.12), 4 (Sections 4.1, 4.3, 4.4, 4.5), 5, 6, 7, 8 and 10; other courses treat material from Chapters 9, 11, 14–17.)
2. Chapter 3 plays a special rôle. The material here is central to combinatorics: subsets, partitions, and permutations of finite sets. Within the other chapters, you are encouraged to dabble, taking or leaving sections as you choose; but I recommend reading all of Chapter 3 (except perhaps the Projects, see below).
3. A number of sections are designated as Projects. These are to be regarded as less central and possibly more difficult than the others. The word suggests that they could be worked through by individuals outside class time, and then made the subject of presentations to the class.
4. Each chapter after this one begins with a box containing 'topics, techniques, algorithms and cross-references'. This is designed to give you some indication of the scope of the chapter. Roughly speaking, topics are specific results or constructions; techniques are of wider applicability, indicating general methods which may be illustrated in specific cases in the chapter; algorithms are self-explanatory; and

cross-references pinpoint at least some occurrences of the material in other chapters. These are usually backward references, but the multidimensional nature of the subject means that this is not always so. You should use these as pointers to places where you might find help if you are stuck on something. The index can also be used for this purpose.

5. The exercises are a mixed bunch; but, by and large, I have tended to avoid 'drill' and give more substantial problems. You will certainly learn more if you work conscientiously through them. But I have tried not to assume that you have done all the problems. When (as often happens) the result of an exercise is needed in a later chapter, I have usually supplied a proof (or, failing that, a hint). Indeed, hints are strewn liberally through the exercises, and some example solutions are given (rather more briefly than I would expect from students!) at the end of the book.

6. The last chapter does two jobs. First, it treats (somewhat sketchily) some further topics not mentioned earlier; second, it gives pointers to further reading in various parts of combinatorics. I have included a small collection of unsolved problems here, to indicate the sort of thing that research in combinatorics might involve. But beware: these problems are unsolved; this means that somebody has given some thought to them and failed to solve them, so they are probably more difficult than the exercises in other chapters.

7. The numbering is as follows. Chapter A is divided into sections, of which a typical one is Section A.B. Within a section, theorems (and similar statements such as propositions, lemmas, corollaries, facts, algorithms, and numbered equations) have numbers of the form A.B.C. On the other hand, diagrams are just numbered within the chapter, as A.D, for example; and exercises are typically referred to as 'exercise E of Chapter A'. Some theorems or facts are displayed in a box for easy reference. But don't read too much into the difference between displayed and undisplayed theorems, or between theorems and propositions; it's a matter of taste, and consistency is not really possible.

8. An important part of combinatorics today is the algorithmic side: I can prove that some object exists; how do I construct it? I have described algorithms for a wide range of constructions. No knowledge of computers or programming languages is assumed. The description of the algorithms makes use of words like 'While ...', 'Repeat ... until ...', and so on. These are to be interpreted as having their usual English meaning. Of course, this meaning has been taken over by programming languages; if you are fluent in Pascal, you will I hope find my descriptions quite congenial. If you are a competent programmer and have access to a computer, you are advised at several places to implement these algorithms.

What you need to know

The mathematical results that I use are listed here. You don't need everything all at once; the more advanced parts of algebra, for example, are only required later in the book, so you could study algebra and combinatorics at the same time. If all else fails, I have tried to arrange things so that you can take on trust what you don't know. Topics in square brackets are treated in the book, but you may feel the

need of more explanation from a course or textbook in that subject. As you see, combinatorics connects with all of mathematics; you will see material from many other areas being used here.

- *Basic pure mathematics*: Sets and functions, ordered n -tuples and cartesian products; integers, factorisation, modular arithmetic; [equivalence and order relations].
- *Linear algebra*: Vector spaces, subspaces; linear transformations, matrices; row operations, row space; eigenvalues of real symmetric matrices.
- *Abstract algebra*: [Elementary group theory; finite fields].
- *Number theory*: [Quadratic residues; two and four squares theorems].
- *Analysis*: Basic operations (limits, differentiation, etc.); [power series].⁴
- *Topology*: [Definition of metric and topological space; surfaces; Jordan curve theorem].
- *Probability*: Basic concepts (for finite spaces only) [except in Chapter 19].
- *Set theory*: See Chapter 19.

Exercises

1. For $n = 3, 4, 5$, calculate the number of ways of putting n letters into their envelopes so that every letter is incorrectly addressed. Calculate the ratio of this number to $n!$ in each case.
2. Solve Kirkman's problem for nine schoolgirls, walking for four days.
3. Solve Euler's problem for nine, sixteen and twenty-five officers. Show that no solution is possible for four officers.
4. Test the assertion that the Ramsey game cannot end in a draw by playing it with a friend. Try to develop heuristic rules for successful play.

⁴ As will be explained in Section 4.2, our treatment of power series is formal and does not involve questions of convergence.

2. On numbers and counting

One of them is all alone and ever more shall be so
Two of them are lily-white boys all clothed all in green Oh
Three of them are strangers o'er the wide world they are rangers
Four it is the Dilly Hour when blooms the Gilly Flower
Five it is the Dilly Bird that's seldom seen but heard
Six it is the ferryman in the boat that o'er the River floats Oh
Seven are the Seven Stars in the Sky, the Shining Stars be Seven Oh
Eight it is the Morning's break when all the World's awake Oh
Nine it is the pale Moonshine, the Shining Moon is Nine Oh
Ten Forgives all kinds of Sin, from Ten begin again Oh

English traditional folksong
from Bob Stewart, *Where is Saint George?* (1977)

TOPICS: Natural numbers and their representation; induction; useful functions; rates of growth; counting labelled and unlabelled structures; Handshaking Lemma

TECHNIQUES: Induction; double counting

ALGORITHMS: Odometer Principle; [Russian peasant multiplication]

CROSS-REFERENCES:

This chapter is about counting. In some sense, it is crucial to what follows, since counting is so basic in combinatorics. But this material is part of mathematical culture, so you will probably have seen most of it before.

2.1. Natural numbers and arithmetic

Kronecker is often quoted as saying about mathematics, 'God made the integers; the rest is the work of man.' He was referring to the natural numbers (or counting numbers), which are older than the earliest archæological evidence. (Zero and the negative numbers are much more recent, having been invented (or discovered) in historical time.)¹ Since much of combinatorics is concerned with counting, the natural numbers have special significance for us.

¹ See Georges Ifrah, *From One to Zero: A Universal History of Numbers* (1985), for an account of the development of numbers and their representation.

As each new class of numbers was added to the mathematical repertoire, it was given a name reflecting the prejudice against its members, or the 'old' numbers were given a friendly, reassuring name. Thus, zero and negative integers are contrasted with the 'natural' positive integers. Later, quotients of integers were 'rational', as opposed to the 'irrational' square root of 2; and later still, all numbers rational and irrational were regarded as 'real', while the square root of -1 was 'imaginary' (and its friends were 'complex').

The natural numbers are the first mathematical construct with which we become familiar. Small children recite the names of the first few natural numbers in the same way that they might chant a nursery rhyme or playground jingle. This gives them the concept that the numbers come in a sequence. They grasp this in a sophisticated way. The rhyme²

One, two,
Missed a few,
Ninety-nine,
A hundred

expresses confidence that the sequence of numbers stretches at least up to 100, and that the speaker could fill in the gap if pressed.

Order or progression is thus the most basic property of the natural numbers.³ How is this expressed mathematically? First we must stop to consider how natural numbers are represented. The simplest way to represent the number n is by a sequence of n identical marks. This is probably the earliest scheme mankind adopted. It is well adapted for tallying: to move from one number to the next, simply add one more mark. However, large numbers are not easily recognisable. After various refinements (ranging from grouping the marks in sets of five to the complexities of Roman numerals), positional notation was finally adopted.

This involves the choice of a base b (an integer greater than 1), and b digits (distinguishable symbols for the integers $0, 1, 2, \dots, b-1$). (Early attempts at positional notation were bedevilled because the need for a symbol for zero was not recognised.) Now any natural number N is represented by a finite string of digits. Logically the string is read from right to left; so we write it as $x_{n-1} \dots x_1 x_0$, where each x_i is one of our digits. By convention, the leftmost digit is never zero. The algorithm for advancing to the next number is called the *Odometer Principle*. It is based on the principle of trading in b counters in place i for a single counter in place $i+1$, and should be readily understood by anyone who has watched the odometer (or mileage gauge) of a car.

² I have heard the feminist version of this: 'One, two, Mrs. Few, ...'

³ 'The operations of arithmetic are based on the tacit assumption that we can always pass from any number to its successor, and this is the essence of the ordinal concept.' Tobias Dantzig, *Number: the Language of Science* (1930).

(2.1.1) Odometer Principle

to find the successor of a natural number to base b

Start by considering the rightmost digit.

- *If the digit we are considering is not $b - 1$, then replace it by the next digit in order, and terminate the algorithm.*
- *If we are considering a blank space (to the left of all the digits), then write in it the digit 1, and terminate the algorithm.*
- *If neither of the above holds, we are considering the digit $b - 1$. Replace it with the digit 0, move one place left, and return to the first bullet point.*

For example, if the base b is 2 and the digits are 0 and 1, the algorithm (starting with 1) generates successively 10, 11, 100, 101, 110, ...

Now it can be proved by induction that the string $x_{n-1} \dots x_1 x_0$ represents the positive integer

$$x_{n-1}b^{n-1} + \dots + x_1b + x_0$$

(see Exercise 2).

Often the number 0 is included as a natural number. (This is most usually done by logicians, who like to generate the whole number system out of zero, or nothing. But it conflicts with our childhood experience: I have never heard a child say 'nought, one, two, ...'⁴, and we don't count that way.) This is done by modifying our representation so that the digit 0 represents the number 0. This is the one allowed exception to the rule that the left-most digit cannot be 0; the alternative, representing 0 by a blank space, would be confusing.

The odometer of a car actually works slightly differently. It works with a fixed number of digits which are initially all zero, so that the 'blank space' case of the algorithm cannot arise. If there are k digits, then the integers $0, \dots, b^k - 1$ are generated in turn, and then the odometer returns to 0 and the process repeats.

Now that we have a representation of positive integers, and understand how to move to the next integer, we should explore the arithmetic operations (ambition, distraction, uglification and derision).⁵ Algorithms for these are taught in primary school.⁶ I will not consider the details here. It is a good exercise to program a computer to perform these algorithms⁷, or to investigate how many elementary

⁴ A possible exception occurs when one child has been appointed to be first, and another wishes to claim precedence, as in 'Zero the hero'. But this is closer to the historical than the logical approach.

⁵ Lewis Carroll, *Alice's Adventures in Wonderland* (1865).

⁶ These algorithms were known to the Babylonians in 1700 B.C.

⁷ Most programming languages specify the 'maximum integer' to be something like 32767 or 2147483647. Often, the answer to a counting problem will be much larger than this. To find it by computer, you may have to write routines for arithmetic operations on integers with many digits. If you need to do this, write your routines so that you can re-use them!

operations are required to add or multiply two n -digit numbers (where elementary operations might consist of referring to one's memory of the multiplication tables, or writing down a digit).

2.2. Induction

Induction is a very powerful principle for proving assertions about the natural numbers. It is applied in various different forms, some of which are described in this section. We also see that it is a consequence of our most basic intuition about the natural numbers.

The *Principle of Induction* asserts the following:

(2.2.1) Principle of Induction

Let $P(n)$ be a proposition or assertion about the natural number n . Suppose that $P(1)$ is true. Suppose also that, if $P(n)$ is true, then $P(n+1)$ is also true. Then $P(n)$ is true for all natural numbers n .

Why is this true? As we saw, the basic property of the natural numbers, recognised even by children, is that we can count up to any natural number n starting from 1 (given sufficient patience!) Now, with the assumptions of the Principle, $P(1)$ is true, so $P(2)$ is true, so (miss a few here) so $P(n-1)$ is true, so $P(n)$ is true.

As this argument suggests, if you are reading a mathematical argument, and the author puts in a few dots or the words 'and so on', there is probably a proof by induction hiding there. Consider, for example, the function f satisfying $f(1) = 2$ and $f(n+1) = 2f(n)$ for all natural numbers n . Then

$$f(2) = 4 = 2^2, f(3) = 8 = 2^3, \quad \dots \quad f(n) = 2^n.$$

The dots hide a proof by induction. Let $P(n)$ be the assertion that $f(n) = 2^n$. Then $P(1)$ holds; and, assuming that $P(n)$ holds, we have

$$P(n+1) = 2P(n) = 2 \cdot 2^n = 2^{n+1},$$

so $P(n+1)$ also holds. So the Principle of Induction justifies the conclusion. The point is that very simple arguments by induction can be written out with three dots in place of the detailed verification, but this verification could be supplied if necessary. We'll see more examples of this later.

Now I give some alternative forms of the Principle of Induction and justify their equivalence. The first one is transparent. Suppose that $P(n)$ is an assertion, for which we know that $P(27)$ is true, and that if $P(n)$ holds then so does $P(n+1)$. Then we conclude that $P(n)$ holds for all $n \geq 27$. (To prove this formally, let $Q(n)$ be the assertion that $P(n+26)$ is true, and verify the hypotheses of the Principle of Induction for $Q(n)$.)

For the next variation, let $P(n)$ be a proposition about natural numbers. Suppose that, for every natural number n , if $P(m)$ holds for all natural numbers m less than