Discrete Mathematics Notes

David A. SANTOS
dsantos@ccp.edu

January 2, 2010 REVISION

Contents

Preface

These notes started in the Spring of 2004, but contain material that I have used in previous years.

I would appreciate any comments, suggestions, corrections, etc., which can be addressed at the email below.

David A. Santos
dsantos@ccp.edu

Things to do:

- Weave functions into counting, *à la twelfold way*. . .

GNU Free Documentation License

Preamble

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "**Document**", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "**you**". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "**Modified Version**" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "**Secondary Section**" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "**Invariant Sections**" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "**Cover Texts**" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "**Transparent**" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "**Opaque**".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "**Title Page**" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "**Entitled XYZ**" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "**Acknowledgements**", "**Dedications**", "**Endorsements**", or "**History**".) To "**Preserve the Title**" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties–for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

Chapter 1

Pseudocode

In this chapter we study pseudocode, which will allow us to mimic computer language in writing algorithms.

1.1 Operators

1 Definition (Operator) An *operator* is a character, or string of characters, used to perform an action on some entities. These entities are called the *operands.*

2 Definition (Unary Operators) A *unary operator* is an operator acting on a single operand.

Common arithmetical unary operators are $+$ (plus) which indicates a positive number, and $-$ (minus) which indicates a negative number.

3 Definition (Binary Operators) A *binary operator* is an operator acting on two operands.

Common arithmetical binary operators that we will use are $+$ (plus) to indicate the sum of two numbers and $-$ (minus) to indicate a difference of two numbers. We will also use $*$ (asterisk) to denote multiplication and $/$ (slash) to denote division.

There is a further arithmetical binary operator that we will use.

4 Definition (mod Operator) The operator $\mod$ is defined as follows: for $a \geq 0$, $b > 0$,

$$a \mod b$$

is the integral non-negative remainder when a is divided by b. Observe that this remainder is one of the b numbers

$$0, \quad 1, \quad 2, \quad \ldots, \quad b-1.$$

In the case when at least one of a or b is negative, we will leave $a \mod b$ undefined.

5 Example We have

$$38 \mod 15 = 8,$$

$$15 \mod 38 = 15,$$

$$1961 \mod 37 = 0,$$

and

$$1966 \mod 37 = 5,$$

for example.

6 Definition (Precedence of Operators) The priority or *precedence* of an operator is the order by which it is applied to its operands. Parentheses ( ) are usually used to coerce precedence among operators. When two or more operators of the same precedence are in an expression, we define the *associativity* to be the order which determines which of the operators will be executed first. *Left-associative* operators are executed from left to right and *right-associative* operators are executed from right to left.

Recall from algebra that multiplication and division have the same precedence, and their precedence is higher than addition and subtraction. The mod operator has the same precedence as multiplication and addition. The arithmetical binary operators are all left associative whilst the arithmetical unary operators are all right associative.

7 Example $15-3*4=3$ but $(15-3)*4=48$.

8 Example $12*(5 \mod 3)=24$ but $(12*5) \mod 3=0$.

9 Example $12 \mod 5+3*3=11$ but $12 \mod (5+3)*3=12 \mod 8*3=4*3=12$.

1.2 Algorithms

In pseudocode parlance an *algorithm* is a set of instructions that accomplishes a task in a finite amount of time. If the algorithm produces a single output that we might need afterwards, we will use the word **return** to indicate this output.

10 Example (Area of a Trapezoid) Write an algorithm that gives the area of a trapezoid whose height is h and bases are a and b.

Solution: One possible solution is

Algorithm 1.2.1: AREATRAPEZOID(a,b,h)

return $(h*\left(\frac{a+b}{2}\right))$

11 Example (Heron's Formula) Write an algorithm that will give the area of a triangle with sides a, b, and c.

Solution: A possible solution is

Algorithm 1.2.2: AREAOFTRIANGLE(a,b,c)

return $(.25*\sqrt{(a+b+c)*(b+c-a)*(c+a-b)*(a+b-c)})$

We have used Heron's formula

$$\text{Area } = \sqrt{s(s-a)(s-b)(s-c)} = \frac{1}{4}\sqrt{(a+b+c)(b+c-a)(c+a-b)(a+b-c)},$$

where

$$s = \frac{a+b+c}{2}$$

is the semi-perimeter of the triangle.

12 Definition The symbol $\leftarrow$ is read "gets" and it is used to denote assignments of value.

13 Example (Swapping variables) Write an algorithm that will interchange the values of two variables x and y, that is, the contents of x becomes that of y and viceversa.

Solution: We introduce a temporary variable t in order to store the contents of x in y without erasing the contents of y:

Algorithm 1.2.3: SWAP(x,y)

$$\begin{cases} t \leftarrow x & \textbf{comment: } \text{First store } x \text{ in temporary place} \\ x \leftarrow y & \textbf{comment: } x \text{ has a new value.} \\ y \leftarrow t & \textbf{comment: } y \text{ now receives the original value of } x. \end{cases}$$

If we approached the problem in the following manner

Algorithm 1.2.4: SWAPWRONG(x,y)

$$\begin{cases} x \leftarrow 5 & \\ y \leftarrow 6 & \\ x \leftarrow y & \textbf{comment: } x = 6 \text{ now.} \\ y \leftarrow x & \textbf{comment: } y \text{ takes the current value of } x, \text{ i.e., } 6. \end{cases}$$

we do not obtain a swap.

14 Example (Swapping variables 2) Write an algorithm that will interchange the values of two variables x and y, that is, the contents of x becomes that of y and viceversa, *without introducing a third variable*.

Solution: The idea is to use sums and differences to store the variables. Assume that initially $x = a$ and $y = b$.

Algorithm 1.2.5: SWAP2(x,y)

$$\begin{cases} x \leftarrow x+y & \textbf{comment: } x = a+b \text{ and } y = b. \\ y \leftarrow x-y & \textbf{comment: } y = a+b-b = a \text{ and } x = a+b. \\ x \leftarrow x-y & \textbf{comment: } y = a \text{ and } x = a+b-a = b. \end{cases}$$

1.3 Arrays

15 Definition An *array* is an aggregate of homogeneous types. The *length of the array* is the number of entries it has.

A 1-dimensional array is akin to a mathematical vector. Thus if X is 1-dimensional array of length n then

$$X = (X[0], X[1], \ldots, X[n-1])$$

and all the n coordinates $X[k]$ belong to the same set. We will follow the C-C++-Java convention of indexing the arrays from 0. We will always declare the length of the array at the beginning of a code fragment by means of a comment.

A 2-dimensional array is akin to a mathematical matrix. Thus if Y is a 2-dimensional array with 2 rows and 3 columns then

$$Y = \begin{bmatrix} Y[0][0] & Y[0][1] & Y[0][2] \\ Y[1][0] & Y[1][1] & Y[1][2] \end{bmatrix}.$$

1.4 `If-then-else` Statements

16 Definition The **If-then-else** control statement has the following syntax:
if *expression*

$$\textbf{then}\ \begin{cases} statementA-1 \\ \vdots \\ statementA-I \end{cases}$$

$$\textbf{else}\ \begin{cases} statementB-1 \\ \vdots \\ statementB-J \end{cases}$$

and evaluates as follows. If expression is true then all statementA 's are executed. Otherwise all statementB's are executed.

17 Example (Maximum of 2 Numbers) Write an algorithm that will determine the maximum of two numbers.

Solution: Here is a possible approach.

Algorithm 1.4.2: MAX(x,y)

if $x \geq y$
  then return (x)
  else return (y)

18 Example (Maximum of 3 Numbers) Write an algorithm that will determine the maximum of three numbers.

Solution: Here is a possible approach using the preceding function.

Algorithm 1.4.3: MAX3(x,y,z)

if MAX$(x,y) \geq z$
  then return (MAX(x,y))
  else return (z)

19 Example (Compound Test) Write an algorithm that prints "Hello" if one enters a number between 4 and 6 (inclusive) and "Goodbye" otherwise. You are not allowed to use any boolean operators like **and**, **or**, etc.

Solution: Here is a possible answer.

Algorithm 1.4.4: HELLOGOODBYE(x)

if $x >= 4$

$$\textbf{then}\ \begin{cases} \textbf{if}\ x <= 6 \\ \quad \textbf{then output}\ (\text{Hello.}) \\ \quad \textbf{else output}\ (\text{Goodbye.}) \end{cases}$$

  else output (Goodbye.)

1.5 The `for` loop

20 Definition The **for** loop has either of the following syntaxes:[1]
for indexvariable ← lowervalue **to** uppervalue
  do statements
or
for indexvariable ← uppervalue **downto** lowervalue
  do statements
Here lower value and upper value must be non-negative integers with uppervalue ≥ lowervalue.

21 Example (Factorial Integers) Recall that for a non-negative integer n the quantity $n!$ (read "n factorial") is defined as follows. $0! = 1$ and if $n > 0$ then $n!$ is the product of all the integers from 1 to n inclusive:

$$n! = 1 \cdot 2 \cdots n.$$

For example $5! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120$. Write an algorithm that given an arbitrary non-negative integer n outputs $n!$.

Solution: Here is a possible answer.

Algorithm 1.5.3: FACTORIAL(n)

comment: Must input an integer $n \geq 0$.

$f \leftarrow 1$
if $n = 0$
  then return (f)
  else **for** $i \leftarrow 1$ **to** n
    do $f \leftarrow f * i$
return (f)

22 Example (Positive Integral Powers 1) Write an algorithm that will compute x^n, where x is a given real number and n is a given positive integer.

Solution: We can approach this problem as we did the factorial function in example **??**. Thus a possible answer would be

Algorithm 1.5.4: POWER1(x, n)

power ← 1
for $i \leftarrow 1$ **to** n
  do power ← $x *$ power
return (power)

In example **??** we shall examine a different approach.

23 Example (Reversing an Array) An array $(X[0], \ldots X[n-1])$ is given. Without introducing another array, put its entries in reverse order.

Solution: Observe that we exchange

$$X[0] \leftrightarrow X[n-1],$$

$$X[1] \leftrightarrow X[n-2],$$

[1] The syntax in C, C++, and Java is slightly different and makes the **for** loop much more powerful than the one we are presenting here.

and in general

$$X[i] \leftrightarrow X[n-i-1].$$

This holds as long as $i < n-i-1$, that is $2i < n-1$, which happens if and only if $2i \leq n-2$, which happens if and only if $i \leq \lfloor (n-2)/2 \rfloor$. We now use a swapping algorithm, say the one of example **??**.Thus a possible answer is

Algorithm 1.5.5: REVERSEARRAY(n, X)

comment: X is an array of length n.

for $i \leftarrow 0$ **to** $\lfloor (n-2)/2 \rfloor$
  do Swap$(X[i], X[n-i-1])$

24 Definition The command **break** stops the present control statement and jumps to the next control statement. The command **output(...)** prints whatever is enclosed in the parentheses.

☞ *Many a programmer considers using the* **break** *command an ugly practice. We will use it here and will abandon it once we study the* **while** *loop.*

25 Example What will the following algorithm print?

Algorithm 1.5.6: PRINTING$(\cdot)$

for $i \leftarrow 3$ **to** 11
  do **if** $i = 7$
    then break
    else output (i)

Solution: We have, in sequence,

❶ $i = 3$. Since $3 \neq 7$, the programme prints 3.

❷ $i = 4$. Since $4 \neq 7$, the programme prints 4.

❸ $i = 5$. Since $5 \neq 7$, the programme prints 5.

❹ $i = 6$. Since $6 \neq 7$, the programme prints 6.

❺ $i = 7$. Since $7 = 7$, the programme halts and nothing else is printed.

The programme ends up printing 3456.

26 Example (Maximum of n Numbers) Write an algorithm that determines the maximum element of a 1-dimensional array of n elements.

Solution: We declare the first value of the array (the 0-th entry) to be the maximum (a *sentinel value*). Then we successively compare it to other $n-1$ entries. If an entry is found to be larger than it, that entry is declared the maximum.

Algorithm 1.5.7: MAXENTRYINARRAY(n, X)

comment: X is an array of length n.

max $\leftarrow X[0]$
for $i \leftarrow 1$ **to** $n-1$
  do **if** $X[i] >$ max
    then max $= X[i]$
return (max)

Recall that a positive integer $p > 1$ is a *prime* if its only positive factors of p are either 1 or p. An integer greater than 1 which is not prime is said to be *composite*.[2] To determine whether an integer is prime we rely on the following result.

27 Theorem Let $n > 1$ be a positive integer. Either n is prime or n has a prime factor $\leq \sqrt{n}$.

> **Proof:** *If n is prime there is nothing to prove. Assume then than n is composite. Then n can be written as the product* $n = ab$ *with* $1 < a \leq b$. *If every prime factor of n were* $> \sqrt{n}$ *then we would have both* $a > \sqrt{n}$ *and* $b > \sqrt{n}$ *then we would have* $n = ab > \sqrt{n}\sqrt{n} = n$, *which is a contradiction. Thus n must have a prime factor* $\leq \sqrt{n}$. ❑

28 Example To determine whether 103 is prime we proceed as follows. Observe that $\lfloor \sqrt{103} \rfloor = 10$.[3] We now divide 103 by every prime ≤ 10. If one of these primes divides 103 then 103 is not a prime. Otherwise, 103 is a prime. A quick division finds

$$\begin{aligned} 103 \mod 2 &= 1, \\ 103 \mod 3 &= 1, \\ 103 \mod 5 &= 3, \\ 103 \mod 7 &= 5, \end{aligned}$$

whence 103 is prime since none of these remainders is 0.

29 Definition (Boolean Variable) A *boolean variable* is a variable that only accepts one of two possible values: **true** or **false**.

The **not** unary operator changes the status of a boolean variable from **true** to **false** and viceversa.

30 Example (Eratosthenes' Primality Testing) Given a positive integer n write an algorithm to determine whether it is prime.

Solution: Here is a possible approach. The special cases $n = 1$, $n = 2$, $n = 3$ are necessary because in our version of the **for** loop we need the lower index to be at most the upper index.

Algorithm 1.5.8: ISPRIME1(n)

comment: n is a positive integer.

if $n = 1$
  then output (n is a unit.)
if $n = 2$
  then output (n is prime.)
if $n = 3$
  then output (n is prime.)
comment: If $n \geq 4$, then $\lfloor \sqrt{n} \rfloor \geq 2$.

if $n > 3$
then
  if $n \mod 2 = 0$
    then output (n is even. Its smallest factor is 2.)
  else
    flag $\leftarrow$ **true**
    for $i \leftarrow 2$ **to** $\lfloor \sqrt{n} \rfloor$
      do
        if $n \mod i = 0$
          then
            flag $\leftarrow$ **false**
            break
    if flag $=$ **true**
      then output (n is prime.)
      else output (Not prime. n smallest factor is i.)

[2] Thus 1 is neither prime nor composite.
[3] Here $\lfloor x \rfloor$ denotes the floor of x, that is, the integer just to the left of x if x is not an integer and x otherwise.

☞ *From a stylistic point of view, this algorithm is unsatisfactory, as it uses the* **break** *statement. We will see in example* **??** *how to avoid it.*

31 Example (The Locker-room Problem) A locker room contains n lockers, numbered 1 through n. Initially all doors are open. Person number 1 enters and closes all the doors. Person number 2 enters and opens all the doors whose numbers are multiples of 2. Person number 3 enters and if a door whose number is a multiple of 3 is open then he closes it; otherwise he opens it. Person number 4 enters and changes the status (from open to closed and viceversa) of all doors whose numbers are multiples of 4, and so forth till person number n enters and changes the status of door number n. Write an algorithm to determine which lockers are closed.

Solution: Here is one possible approach. We use an array `Locker` of size $n+1$ to denote the lockers (we will ignore `Locker[0]`). The value **true** will denote an open locker and the value **false** will denote a closed locker.[4]

Algorithm 1.5.9: LOCKERROOMPROBLEM(n, *Locker*)

comment: *Locker* is an array of size $n+1$.

comment: Closing all lockers in the first for loop.

for $i \leftarrow 1$ **to** n
  do $Locker[i] \leftarrow$ **false**
comment: From open to closed and vice-versa in the second loop .

for $j \leftarrow 2$ **to** n
  do { **for** $k \leftarrow j$ **to** n
    do if $k \mod j = 0$
    then $Locker[k] =$ **not** $Locker[k]$
for $l \leftarrow 1$ **to** n
  do { **if** $Locker[l] =$ **false**
    then output (Locker l is closed.)

1.6 The `while` loop

32 Definition The **while** loop has syntax:
while test
  do {body of loop
The commands in the body of the loop will be executed as long as `test` evaluates to true.

33 Example (Different Elements in an Array) An array X satisfies $X[0] \leq X[1] \leq \cdots \leq X[n-1]$. Write an algorithm that finds the number of entries which are different.

Solution: Here is one possible approach.

Algorithm 1.6.2: DIFFERENT(n, X)

comment: X is an array of length n.

$i \leftarrow 0$
different $\leftarrow 1$
while $i \neq n-1$
  do { $i \leftarrow i+1$
    if $x[i] \neq x[i-1]$
    then different $\leftarrow$ different $+1$
return (different)

[4] We will later see that those locker doors whose numbers are squares are the ones which are closed.

34 Example (Positive Integral Powers 2) Write an algorithm that will compute a^n, where a is a given real number and n is a given positive integer.

Solution: We have already examined this problem in example **??**. From the point of view of computing time, that solution is unsatisfactory, as it would incur into n multiplications, which could tax the computer memory if n is very large. A more efficient approach is the following. Basically it consists of writing n in binary. We successively square x getting a sequence

$$x \to x^2 \to x^4 \to x^8 \to \cdots \to x^{2^k},$$

and we stop when $2^k \leq n < 2^{k+1}$. For example, if $n = 11$ we compute $x \to x^2 \to x^4 \to x^8$. We now write $11 = 8+2+1$ and so $x^{11} = x^8 x^2 x$.

Algorithm 1.6.3: POWER2(x,n)

power $\leftarrow 1$
$c \leftarrow x$
$k \leftarrow n$
while $k \neq 0$
do { **if** $k \mod 2 = 0$
  then { $k \leftarrow k/2$; $c \leftarrow c * c$
  else { $k \leftarrow k-1$; power $\leftarrow$ power $* c$
return (power)

The **while** loop can be used to replace the **for** loop, and in fact, it is more efficient than it. For, the code **for** $i \leftarrow k$ **to** n **do** something

is equivalent to

$i \leftarrow k$
while $i <= n$
do { $i \leftarrow i+1$; something

But more can be achieved from the **while** loop. For instance, instead of jumping the index one-step-at-a-time, we could jump t steps at a time by declaring $i \leftarrow i+t$. Also, we do not need to use the **break** command if we incorporate the conditions for breaking in the test of the loop.

35 Example Here is the ISPRIME1 programme from example **??** with **while** loops replacing the **for** loops. If $n > 3$, then n is divided successively by odd integers, as it is not necessary to divide it by even integers.

Algorithm 1.6.6: IsPrime2(n)

comment: n is a positive integer.

if $n = 1$
  then output (n is a unit.)
if $n = 2$
  then output (n is prime.)
if $n = 3$
  then output (n is prime.)
if $n > 3$
  then
    if $n \mod 2 = 0$
      then output (n is even. Its smallest factor is 2.)
      else
        flag $\leftarrow$ **true**
        $i \leftarrow 1$
        while $i <= \lfloor \sqrt{n} \rfloor$ **and** flag $=$ **true**
          do
            $i \leftarrow i + 2$
            if $n \mod i = 0$
              then flag $\leftarrow$ **false**
        if flag $=$ **true**
          then output (n is prime.)
          else output (Not prime. n smallest factor is i.)

Homework

36 Problem What will the following algorithm return for $n = 5$? You must trace the algorithm carefully, outlining all your steps.

Algorithm 1.6.7: Mystery(n)

$x \leftarrow 0$
$i \leftarrow 1$
while $n > 1$
  do
    if $n * i > 4$
      then $x \leftarrow x + 2n$
      else $x \leftarrow x + n$
    $n \leftarrow n - 2$
    $i \leftarrow i + 1$
return (x)

37 Problem What will the following algorithm return for $n = 3$?

Algorithm 1.6.8: Mystery(n)

$x \leftarrow 0$
while $n > 0$
  do
    for $i \leftarrow 1$ **to** n
      do
        for $j \leftarrow i$ **to** n
          do $x \leftarrow ij + x$
    $n \leftarrow n - 1$
return (x)

38 Problem Assume that the division operator / acts as follows on the integers: if the division is not even, a/b truncates the decimal part of the quotient. For example $5/2 = 2$, $5/3 = 1$. Assuming this write an algorithm that reverses the digits of a given integer. For example, if 123476 is the input, the output should be 674321. Use only one `while` loop, one mod operation, one multiplication by 10 and one division by 10.

39 Problem Given is an array of length $m+n$, which is sorted in increasing order:

$$X[0] < X[1] < \ldots < X[m-1] < X[m] < \ldots < X[m+n-1].$$

Without using another array reorder the array in the form

$$X[m] \to X[m+1] \to \ldots \to X[m+n-1] \to X[0] \to X[1] \to \ldots \to X[m-1].$$

Do this using algorithm REVERSEARRAY from example **??** a few times.

40 Problem The *Fibonacci Sequence* is defined recursively as follows:

$$f_0 = 0; \quad f_1 = 1, \quad f_2 = 1, \quad f_{n+1} = f_n + f_{n-1}, n \geq 1.$$

Write an algorithm that finds the n-th Fibonacci number.

41 Problem Write an algorithm which reads a sequence of real numbers and determines the length of the longest non-decreasing subsequence. For instance, in the sequence

$$7,8,7,8,9,2,1,8,7,9,9,10,10,9,$$

the longest non-decreasing subsequence is $7,9,9,10,10$, of length 5.

42 Problem Write an algorithm that reads an array of n integers and finds the second smallest entry.

43 Problem A *partition* of the strictly positive integer n is the number of writing n as the sum of strictly positive summands, without taking the order of the summands into account. For example, the partitions of 4 are (in "alphabetic order" and with the summands written in decreasing order)

$$1+1+1+1; 2+1+1; 3+1; 2+2; 4.$$

Write an algorithm to generate all the partitions of a given integer n.

Answers

36 In the first turn around the loop, $n = 5, i = 1$, $n*i > 4$ and thus $x = 10$. Now $n = 3$, $i = 2$, and we go a second turn around the loop. Since $n*i > 4$, $x = 10+2*3 = 16$. Finally, $n = 1, i = 3$, and the loop stops. Hence $x = 16$ is returned.

38 Here is a possible approach.

Algorithm 1.6.9: REVERSE(n)

comment: n is a positive integer.

$x \leftarrow 0$
while $n \neq 0$
do
- **comment:** x accumulates truncated digit.
- $x \leftarrow x*10+n \mod 10$
- **comment:** We now truncate a digit of the input.
- $n \leftarrow n/10$

return (x)

39 Reverse the array first as

$$X[m+n-1] > X[m+n-2] > \ldots > X[m] > X[m-1] > \ldots > X[0].$$

Then reverse each one of the two segments:

$$X[m] \to X[m+1] \to \ldots \to X[m+n-1] \to X[0] \to X[1] \to \ldots \to X[m-1].$$

40 Here is a possible solution.

Algorithm 1.6.10: FIBONACCI(n)

```
if n = 0
  then return (0)
  else { last ← 0
       { current ← 1
for i ← 2 to n
{ temp ← last + current
{ last ← current
{ current ← temp
return (current)
```

41 Assume that the data is read from some file f. **eof** means "end of file." *newEl* and *oldEl* are the current and the previous elements. d is the length of the current run of non-decreasing numbers. *dMax* is the length of the longest run.

Algorithm 1.6.11: LARGESTINCREASINGSEQUENCE(f)

```
1 ← d
1 ← dMax
while not eof
do { if newEl >= oldEl
   { then { d ← d + 1
          { else { if d > dMax
                 { then dMax ← d
                 { d ← 1
   { oldEl ← newEL
if d > dMax
  then dMax ← d
```

42 Here is one possible approach.

Algorithm 1.6.12: SECONDSMALLEST(n, X)

```
comment: X is an array of length n.
second ← x[0]
minimum ← second
for i ← 0 to n − 1
do { if minimum = second
   { then { if X[i] < minimum
          { then minimum ← X[i]
          { else second ← X[i]
   { else { if X[i] < minimum
          { then { second ← minimum
                 { minimum ← X[i]
          { else { if X[i] > minimum and X[i] < second
                 { then second ← X[i]
```

43 We list partitions of n in alphabetic order and with decreasing summands. We store them in an array of length $n+1$ with $X[0] = 0$.. The length of the partition is k and the summands are $X[1] + \cdots + X[k]$. Initially $k = n$ and $X[1] = \cdots = X[n] = 1$. At the end we have $X[1] = n$ and the rest are 0.

Algorithm 1.6.13: PARTITIONS(n)

$s \leftarrow k-1$
while not $((s=1)$ **or** $(X[s-1] > X[s]))$
$\{ s \leftarrow s-1$
$X[s] \leftarrow X[s]+1$
$\text{sum} \leftarrow 0$
for $i \leftarrow s+1$ **to** k
$\{ \text{sum} \leftarrow \text{sum} + X[i]$
for $i \leftarrow 1$ **to** $\text{sum}-1$
$\{ X[s+i] \leftarrow 1$
$k \leftarrow s+\text{sum}-1$

Chapter 2

Proof Methods

2.1 Proofs: Direct Proofs

A direct proof is one that follows from the definitions. Facts previously learned help many a time when making a direct proof.

44 Example Recall that

- an even number is one of the form $2k$, where k is an integer.
- an odd integer is one of the form $2l+1$ where l is an integer.
- an integer a is divisible by an integer b if there exists an integer c such that $a = bc$.

Prove that

❶ the sum of two even integers is even,

❷ the sum of two odd integers is even,

❸ the sum of an even integer with and odd integer is odd,

❹ the product of two even integers is divisible by 4,

❺ the product of two odd integers is odd,

❻ the product of an even integer and an odd integer is even.

Solution: We argue from the definitions. We assume as known that the sum of two integers is an integer.

❶ If $2a$ and $2b$ are even integers, then $2a+2b = 2(a+b)$, Now $a+b$ is an integer, so $2(a+b)$ is an even integer.

❷ If $2c+1$ and $2d+1$ are odd integers, then $2c+1+2d+1 = 2(c+d+1)$, Now $c+d+1$ is an integer, so $2(c+d+1)$ is an even integer.

❸ Let $2f$ be an even integer and $2g+1$ be an odd integer. Then $2f+2g+1 = 2(f+g)+1$. Since $f+g$ is an integer, $2(f+g)+1$ is an odd integer.

❹ Let $2h$ $2k$ be even integers. Then $(2h)(2k) = 4(hk)$. Since hk is an integer, $4(hk)$ is divisible by 4.

❺ Let $2l+1$ and $2m+1$ be odd integers. Then

$$(2l+1)(2m+1) = 4ml+2l+2m+1 = 2(2ml+l+m)+1.$$

Since $2ml+l+n$ is an integer, $2(2ml+m+l)+1$ is an odd integer.

❻ Let $2n$ be an even integer and let $2o+1$ be an odd integer. Then $(2n)(2o+1) = 4no+2n = 2(2no+1)$. Since $2no+1$ is an integer, $2(2no+1)$ is an even integer.

45 Example Prove that if n is an integer, then n^3-n is always divisible by 6.

Solution: We have $n^3-n = (n-1)n(n+1)$, the product of three consecutive integers. Among three consecutive integers there is at least an even one, and exactly one of them which is divisible by 3. Since 2 and 3 do not have common factors, 6 divides the quantity $(n-1)n(n+1)$, and so n^3-n is divisible by 6.

46 Example Use the fact that the square of any real number is non-negative in order to prove the *Arithmetic Mean-Geometric Mean Inequality:* $\forall x \geq 0, \forall y \geq 0$

$$\sqrt{xy} \leq \frac{x+y}{2}.$$

Solution: First observe that $\sqrt{x} - \sqrt{y}$ is a real number, since we are taking the square roots of non-negative real numbers. Since the square of any real number is greater than or equal to 0 we have

$$(\sqrt{x} - \sqrt{y})^2 \geq 0.$$

Expanding

$$x - 2\sqrt{xy} + y \geq 0 \implies \frac{x+y}{2} \geq \sqrt{xy},$$

yielding the result.

47 Example Prove that a sum of two squares of integers leaves remainder 0, 1 or 2 when divided by 4.

Solution: An integer is either even (of the form $2k$) or odd (of the form $2k+1$). We have

$$\begin{array}{rcl} (2k)^2 & = & 4k^2, \\ (2k+1)^2 & = & 4(k^2+k)+1. \end{array}$$

Thus squares leave remainder 0 or 1 when divided by 4 and hence their sum leave remainder 0, 1, or 2.

2.2 Proofs: Mathematical Induction

The Principle of Mathematical Induction is based on the following fairly intuitive observation. Suppose that we are to perform a task that involves a certain number of steps. Suppose that these steps must be followed in strict numerical order. Finally, suppose that we know how to perform the n-th task provided we have accomplished the $n-1$-th task. Thus if we are ever able to start the job (that is, if we have a base case), then we should be able to finish it (because starting with the base case we go to the next case, and then to the case following that, etc.).

Thus in the Principle of Mathematical Induction, we try to verify that some assertion $P(n)$ concerning natural numbers is true for some base case k_0 (usually $k_0 = 1$). Then we try to settle whether information on $P(n-1)$ leads to favourable information on $P(n)$.

48 Theorem Principle of Mathematical Induction If a set $\mathscr{S}$ of positive integers contains the integer 1, and also contains the integer $n+1$ whenever it contains the integer n, then $\mathscr{S} = \mathbb{N}$.

The following versions of the Principle of Mathematical Induction should now be obvious.

49 Corollary If a set $\mathscr{A}$ of positive integers contains the integer m and also contains $n+1$ whenever it contains n, where $n > m$, then $\mathscr{A}$ contains all the positive integers greater than or equal to m.

50 Corollary (Strong Induction) If a set $\mathscr{A}$ of positive integers contains the integer m and also contains $n+1$ whenever it contains $m+1, m+2, \ldots, n$, where $n > m$, then $\mathscr{A}$ contains all the positive integers greater than or equal to m.

We shall now give some examples of the use of induction.

51 Example Prove that the expression

$$3^{3n+3} - 26n - 27$$

is a multiple of 169 for all natural numbers n.

Solution: Let $P(n)$ be the assertion "$\exists T \in \mathbb{N}$ with $3^{3n+3} - 26n - 27 = 169T$." We will prove that $P(1)$ is true and that $P(n-1) \implies P(n)$. For $n = 1$ we are asserting that $3^6 - 53 = 676 = 169 \cdot 4$ is divisible by 169, which is evident.

Now, $P(n-1)$ means there is $N \in \mathbb{N}$ such that $3^{3(n-1)+3} - 26(n-1) - 27 = 169N$, i.e., for $n > 1$,

$$3^{3n} - 26n - 1 = 169N$$

for some integer N. Then

$$3^{3n+3} - 26n - 27 = 27 \cdot 3^{3n} - 26n - 27 = 27(3^{3n} - 26n - 1) + 676n$$

which reduces to

$$27 \cdot 169N + 169 \cdot 4n,$$

which is divisible by 169. The assertion is thus established by induction.

52 Example Prove that $2^n > n,\ \forall n \in \mathbb{N}$.

Solution: The assertion is true for $n = 0$, as $2^0 > 0$. Assume that $2^{n-1} > n-1$ for $n > 1$. Now,

$$2^n = 2(2^{n-1}) > 2(n-1) = 2n-2 = n+n-2.$$

Now, $n-1 > 0 \implies n-2 \geq 0$, we have $n+n-2 \geq n+0 = n$, and so,

$$2^n > n.$$

This establishes the validity of the n-th step from the preceding step and finishes the proof.

53 Example Prove that

$$(1+\sqrt{2})^{2n} + (1-\sqrt{2})^{2n}$$

is an even integer and that

$$(1+\sqrt{2})^{2n} - (1-\sqrt{2})^{2n} = b\sqrt{2}$$

for some positive integer b, for all integers $n \geq 1$.

Solution: We proceed by induction on n. Let $P(n)$ be the proposition: "$(1+\sqrt{2})^{2n} + (1-\sqrt{2})^{2n}$ is even and $(1+\sqrt{2})^{2n} - (1-\sqrt{2})^{2n} = b\sqrt{2}$ for some $b \in \mathbb{N}$." If $n = 1$, then we see that

$$(1+\sqrt{2})^2 + (1-\sqrt{2})^2 = 6,$$

an even integer, and

$$(1+\sqrt{2})^2 - (1-\sqrt{2})^2 = 4\sqrt{2}.$$

Therefore $P(1)$ is true. Assume that $P(n-1)$ is true for $n > 1$, i.e., assume that

$$(1+\sqrt{2})^{2(n-1)} + (1-\sqrt{2})^{2(n-1)} = 2N$$

for some integer N and that

$$(1+\sqrt{2})^{2(n-1)} - (1-\sqrt{2})^{2(n-1)} = a\sqrt{2}$$

for some positive integer a.

Consider now the quantity

$$(1+\sqrt{2})^{2n} + (1-\sqrt{2})^{2n} = (1+\sqrt{2})^2(1+\sqrt{2})^{2n-2} + (1-\sqrt{2})^2(1-\sqrt{2})^{2n-2}.$$

This simplifies to

$$(3+2\sqrt{2})(1+\sqrt{2})^{2n-2} + (3-2\sqrt{2})(1-\sqrt{2})^{2n-2}.$$

Using $P(n-1)$, the above simplifies to

$$12N + 2\sqrt{2}a\sqrt{2} = 2(6N+2a),$$

an even integer and similarly

$$(1+\sqrt{2})^{2n} - (1-\sqrt{2})^{2n} = 3a\sqrt{2} + 2\sqrt{2}(2N) = (3a+4N)\sqrt{2},$$

and so $P(n)$ is true. The assertion is thus established by induction.

54 Example Prove that if k is odd, then 2^{n+2} divides

$$k^{2^n} - 1$$

for all natural numbers n.

Solution: The statement is evident for $n = 1$, as $k^2 - 1 = (k-1)(k+1)$ is divisible by 8 for any odd natural number k because both $(k-1)$ and $(k+1)$ are divisible by 2 and one of them is divisible by 4. Assume that $2^{n+2} | k^{2^n} - 1$, and let us prove that $2^{n+3} | k^{2^{n+1}} - 1$. As $k^{2^{n+1}} - 1 = (k^{2^n} - 1)(k^{2^n} + 1)$, we see that 2^{n+2} divides $(k^{2n} - 1)$, so the problem reduces to proving that $2 | (k^{2n} + 1)$. This is obviously true since k^{2n} odd makes $k^{2n} + 1$ even.

55 Example The *Fibonacci Numbers* are given by

$$f_0 = 0,\ f_1 = 1,\ f_{n+1} = f_n + f_{n-1},\quad n \geq 1,$$

that is every number after the second one is the sum of the preceding two. Thus the Fibonacci sequence then goes like

$$0, 1, 1, 2, 3, 5, 8, 13, 21, \ldots.$$

Prove using the Principle of Mathematical Induction, that for integer $n \geq 1$,

$$f_{n-1} f_{n+1} = f_n^2 + (-1)^n.$$

Solution: For $n=1$, we have

$$0\cdot 1 = f_0 f_1 = 1^2 - (1)^1 = f_1^2 - (1)^1,$$

and so the assertion is true for $n=1$. Suppose $n>1$, and that the assertion is true for n, that is

$$f_{n-1}f_{n+1} = f_n^2 + (-1)^n.$$

Using the Fibonacci recursion, $f_{n+2} = f_{n+1} + f_n$, and by the induction hypothesis, $f_n^2 = f_{n-1}f_{n+1} - (-1)^n$. This means that

$$\begin{aligned} f_n f_{n+2} &= f_n(f_{n+1}+f_n) \\ &= f_n f_{n+1} + f_n^2 \\ &= f_n f_{n+1} + f_{n-1}f_{n+1} - (-1)^n \\ &= f_{n+1}(f_n + f_{n-1}) + (-1)^{n+1} \\ &= f_{n+1}f_{n+1} + (-1)^{n+1}, \end{aligned}$$

and so the assertion follows by induction.

56 Example Prove that a given square can be decomposed into n squares, not necessarily of the same size, for all $n = 4,6,7,8,\ldots$.

Solution: A quartering of a subsquare increases the number of squares by three (four new squares are gained but the original square is lost). Figure **??** that $n=4$ is achievable. If n were achievable, a quartering would make $\{n, n+3, n+6, n+9, \ldots\}$ also achievable. We will shew

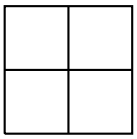

Figure 2.1: Example **??**.

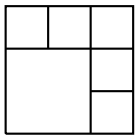

Figure 2.2: Example **??**.

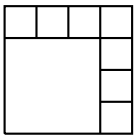

Figure 2.3: Example **??**.

now that $n=6$ and $n=8$ are achievable. But this is easily seen from the figures **??** and **??**, and this finishes the proof.

57 Example In the country of SmallPesia coins only come in values of 3 and 5 pesos. Shew that any quantity of pesos greater than or equal to 8 can be paid using the available coins.

Solution: We use Strong Induction. Observe that $8 = 3+5, 9 = 3+3+3, 10 = 5+5$, so, we can pay $8, 9$, or 10 pesos with the available coinage. Assume that we are able to pay $n-3, n-2$, and $n-1$ pesos, that is, that $3x+5y=k$ has non-negative solutions for $k = n-3, n-2$ and $n-1$. We will shew that we may also obtain solutions for $3x+5y=k$ for $k=n, n+1$ and $n+2$. Now

$$3x+5y = n-3 \Longrightarrow 3(x+1)+5y = n,$$

$$3x_1+5y_1 = n-2 \Longrightarrow 3(x_1+1)+5y_1 = n+1,$$

$$3x_2+5y_2 = n-1 \Longrightarrow 3(x_2+1)+5y_2 = n+2,$$

and so if the amounts $n-3, n-2, n-1$ can be paid so can $n, n+1, n+2$. The statement of the problem now follows from Strong Induction.

2.3 Proofs: Reductio ad Absurdum

In this section we will see examples of proofs by contradiction. That is, in trying to prove a premise, we assume that its negation is true and deduce incompatible statements from this.

58 Example Prove that 2003 is not the sum of two squares by proving that the sum of any two squares cannot leave remainder 3 upon division by 4.

Solution: 2003 leaves remainder 3 upon division by 4. But we know from example **??** that sums of squares do not leave remainder 3 upon division by 4, so it is impossible to write 2003 as the sum of squares.

59 Example Shew, without using a calculator, that $6-\sqrt{35}<\frac{1}{10}$.

Solution: Assume that $6-\sqrt{35}\geq\frac{1}{10}$. Then $6-\frac{1}{10}\geq\sqrt{35}$ or $59\geq 10\sqrt{35}$. Squaring both sides we obtain $3481\geq 3500$, which is clearly nonsense. Thus it must be the case that $6-\sqrt{35}<\frac{1}{10}$.

60 Example Let $a_1,a_2,\ldots,a_n$ be an arbitrary permutation of the numbers $1,2,\ldots,n$, where n is an odd number. Prove that the product

$$(a_1-1)(a_2-2)\cdots(a_n-n)$$

is even.

Solution: First observe that the sum of an odd number of odd integers is odd. It is enough to prove that some difference a_k-k is even. Assume contrariwise that all the differences a_k-k are odd. Clearly

$$S=(a_1-1)+(a_2-2)+\cdots+(a_n-n)=0,$$

since the a_k's are a reordering of $1,2,\ldots,n$. S is an odd number of summands of odd integers adding to the even integer 0. This is impossible. Our initial assumption that all the a_k-k are odd is wrong, so one of these is even and hence the product is even.

61 Example Prove that $\sqrt{2}$ is irrational.

Solution: For this proof, we will accept as fact that any positive integer greater than 1 can be factorised uniquely as the product of primes (up to the order of the factors).

Assume that $\sqrt{2}=\frac{a}{b}$, with positive integers a,b. This yields $2b^2=a^2$. Now both a^2 and b^2 have an even number of prime factors. So $2b^2$ has an odd numbers of primes in its factorisation and a^2 has an even number of primes in its factorisation. This is a contradiction.

62 Example Let a,b be real numbers and assume that for all numbers $\varepsilon>0$ the following inequality holds:

$$a<b+\varepsilon.$$

Prove that $a\leq b$.

Solution: Assume contrariwise that $a>b$. Hence $\frac{a-b}{2}>0$. Since the inequality $a<b+\varepsilon$ holds for every $\varepsilon>0$ in particular it holds for $\varepsilon=\frac{a-b}{2}$. This implies that

$$a<b+\frac{a-b}{2}\ \text{ or }\ a<b.$$

Thus starting with the assumption that $a>b$ we reach the incompatible conclusion that $a<b$. The original assumption must be wrong. We therefore conclude that $a\leq b$.

63 Example (Euclid) Shew that there are infinitely many prime numbers.

Solution: We need to assume for this proof that any integer greater than 1 is either a prime or a product of primes. The following beautiful proof goes back to Euclid.

Assume that $\{p_1,p_2,\ldots,p_n\}$ is a list that exhausts all the primes. Consider the number

$$N=p_1p_2\cdots p_n+1.$$

This is a positive integer, clearly greater than 1. Observe that none of the primes on the list $\{p_1,p_2,\ldots,p_n\}$ divides N, since division by any of these primes leaves a remainder of 1. Since N is larger than any of the primes on this list, it is either a prime or divisible by a prime outside this list. Thus we have shewn that the assumption that any finite list of primes leads to the existence of a prime outside this list. This implies that the number of primes is infinite.

64 Example If a,b,c are odd integers, prove that $ax^2+bx+c=0$ does not have a rational number solution.

Solution: Suppose $\frac{p}{q}$ is a rational solution to the equation. We may assume that p and q have no prime factors in common, so either p and q are both odd, or one is odd and the other even. Now

$$a\left(\frac{p}{q}\right)^2 + b\left(\frac{p}{q}\right) + c = 0 \implies ap^2 + bpq + cq^2 = 0.$$

If both p and p were odd, then $ap^2 + bpq + cq^2$ is also odd and hence $\neq 0$. Similarly if one of them is even and the other odd then either $ap^2 + bpq$ or $bpq + cq^2$ is even and $ap^2 + bpq + cq^2$ is odd. This contradiction proves that the equation cannot have a rational root.

2.4 Proofs: Pigeonhole Principle

The Pigeonhole Principle states that if $n+1$ pigeons fly to n holes, there must be a pigeonhole containing at least two pigeons. This apparently trivial principle is very powerful. Thus in any group of 13 people, there are always two who have their birthday on the same month, and if the average human head has two million hairs, there are at least three people in NYC with the same number of hairs on their head.

The Pigeonhole Principle is useful in proving *existence* problems, that is, we shew that something exists without actually identifying it concretely.

65 Example (Putnam 1978) Let A be any set of twenty integers chosen from the arithmetic progression $1, 4, \ldots, 100$. Prove that there must be two distinct integers in A whose sum is 104.

Solution: We partition the thirty four elements of this progression into nineteen groups

$$\{1\}, \{52\}, \{4, 100\}, \{7, 97\}, \{10, 94\}, \ldots, \{49, 55\}.$$

Since we are choosing twenty integers and we have nineteen sets, by the Pigeonhole Principle there must be two integers that belong to one of the pairs, which add to 104.

66 Example Shew that amongst any seven distinct positive integers not exceeding 126, one can find two of them, say a and b, which satisfy

$$b < a \leq 2b.$$

Solution: Split the numbers $\{1, 2, 3, \ldots, 126\}$ into the six sets

$$\{1, 2\}, \{3, 4, 5, 6\}, \{7, 8, \ldots, 13, 14\}, \{15, 16, \ldots, 29, 30\},$$

$$\{31, 32, \ldots, 61, 62\} \text{ and } \{63, 64, \ldots, 126\}.$$

By the Pigeonhole Principle, two of the seven numbers must lie in one of the six sets, and obviously, any such two will satisfy the stated inequality.

67 Example Given any 9 integers whose prime factors lie in the set $\{3, 7, 11\}$ prove that there must be two whose product is a square.

Solution: For an integer to be a square, all the exponents of its prime factorisation must be even. Any integer in the given set has a prime factorisation of the form $3^a 7^b 11^c$. Now each triplet (a, b, c) has one of the following 8 parity patterns: (even, even, even), (even, even, odd), (even, odd, even), (even, odd, odd), (odd, even, even), (odd, even, odd), (odd, odd, even), (odd, odd, odd). In a group of 9 such integers, there must be two with the same parity patterns in the exponents. Take these two. Their product is a square, since the sum of each corresponding exponent will be even.

Figure 2.4: Example **??**.

Figure 2.5: Example **??**.

68 Example Prove that if five points are taken on or inside a unit square, there must always be two whose distance is $\leq \frac{\sqrt{2}}{2}$.

Solution: Split the square into four congruent squares as shewn in figure **??**. Two of the points must fall into one of the smaller squares, and the longest distance there is, by the Pythagorean Theorem, $\sqrt{(\frac{1}{2})^2+(\frac{1}{2})^2}=\frac{\sqrt{2}}{2}$.

69 Example Fifty one points are placed on and inside a square of side 1. Demonstrate that there must be three of them that fit inside a circle of radius $\frac{1}{7}$.

Solution: Divide the square into 25 congruent squares, as in figure **??**. At least three of the points must fall into one of these mini-squares. Form the circle with centre at the minisquare, and radius of the diagonal of the square, that is, $\frac{1}{5}\cdot\frac{\sqrt{2}}{2}>\frac{1}{7}$, proving the statement.

Homework

70 Problem Prove that if $n>4$ is composite, then n divides $(n-1)!$.

71 Problem Prove that there is no primes triple $p, p+2, p+4$ except for $3,4,5$.

72 Problem If x is an integer and 7 divides $3x+2$ prove that 7 also divides $15x^2-11x-14$.

73 Problem An urn has 900 chips, numbered 100 through 999. Chips are drawn at random and without replacement from the urn, and the sum of their digits is noted. What is the smallest number of chips that must be drawn in order to guarantee that at least three of these digital sums be equal?

74 Problem Let s be a positive integer. Prove that the closed interval $[s;2s]$ contains a power of 2.

75 Problem Let $p<q$ be two *consecutive* odd primes. Prove that $p+q$ is a composite number, having at least three, not necessarily distinct, prime factors.

76 Problem The following 4×4 square has the property that for any of the 16 squares composing it, the sum of the neighbors of that square is 1. For example, the neighbors of a are e and b and so $e+b=1$. Find the sum of all the numbers in the 16 squares.

a	b	c	d
e	f	g	h
i	j	k	l
m	n	o	p

77 Problem Prove, by arguing by contradiction, that there are no integers a,b,c,d such that

$$x^4+2x^2+2x+2=(x^2+ax+b)(x^2+cx+d).$$

78 Problem Let $a>0$. Use mathematical induction to prove that

$$\sqrt{a+\sqrt{a+\sqrt{a+\cdots+\sqrt{a}}}}<\frac{1+\sqrt{4a+1}}{2},$$

where the left member contains an arbitrary number of radicals.

79 Problem Use the AM-GM Inequality: $\forall x\geq 0, \forall y\geq 0,\ \sqrt{xy}\leq\frac{x+y}{2}$ in order to prove that for all quadruplets of non-negative real numbers a,b,c,d we have

$$\sqrt[4]{abcd}\leq\frac{a+b+c+d}{4}.$$

Then, by choosing a special value for d above, deduce that

$$\sqrt[3]{uvw}\leq\frac{u+v+w}{3}$$

for all non-negative real numbers u,v,w.

80 Problem Let a,b,c be real numbers. Prove that if a,b,c are real numbers then

$$a^2+b^2+c^2-ab-bc-ca \geq 0.$$

By direct multiplication, or otherwise, prove that

$$a^3+b^3+c^3-3abc = (a+b+c)(a^2+b^2+c^2-ab-bc-ca).$$

Use the above two results to prove once again that

$$\sqrt[3]{uvw} \leq \frac{u+v+w}{3}$$

for all non-negative real numbers u,v,w.

81 Problem Use the fact that any odd number is of the form $8k\pm 1$ or $8k\pm 3$ in order to give a direct proof that the square of any odd number leaves remainder 1 upon division by 8. Use this to prove that 2001 is not the sum of three odd squares.

82 Problem Find, and prove by induction, the sum of the first n positive odd numbers.

83 Problem Prove by induction that if n non-parallel straight lines on the plane intersect at a common point, they divide the plane into $2n$ regions.

84 Problem Demonstrate by induction that no matter how n straight lines divide the plane, it is always possible to colour the regions produced in two colours so that any two adjacent regions have different colours.

85 Problem Demonstrate by induction that whenever the formula makes sense one has

$$(\cos\theta)(\cos 2\theta)\cdots(\cos 2^n\theta) = \frac{\sin 2^{n+1}\theta}{2^{n+1}\sin\theta}.$$

86 Problem Demonstrate by induction that whenever the formula makes sense one has

$$\sin x+\sin 2x+\cdots+\sin nx = \frac{\sin\frac{n+1}{2}x}{\sin\frac{x}{2}}\cdot\sin\frac{nx}{2}.$$

87 Problem Prove by induction that $2^n > n$ for integer $n \geq 0$.

88 Problem Prove, by induction on n, that

$$1\cdot 2+2\cdot 2^2+3\cdot 2^3+\cdots+n\cdot 2^n = 2+(n-1)2^{n+1}.$$

89 Problem An urn contains 28 blue marbles, 20 red marbles, 12 white marbles, 10 yellow marbles, and 8 magenta marbles. How many marbles must be drawn from the urn in order to assure that there will be 15 marbles of the same color?

90 Problem The nine entries of a 3×3 grid are filled with -1, 0, or 1. Prove that among the eight resulting sums (three columns, three rows, or two diagonals) there will always be two that add to the same number.

91 Problem Forty nine women and fifty one men sit around a round table. Demonstrate that there is at least a pair of men who are facing each other.

92 Problem An eccentric widow has five cats[1]. These cats have 16 kittens among themselves. What is the largest integer n for which one can say that at least one of the five cats has n kittens?

93 Problem No matter which fifty five integers may be selected from

$$\{1,2,\ldots,100\},$$

prove that one must select some two that differ by 10.

[1] Why is it always eccentric widows who have multiple cats?

94 Problem (AHSME 1994) Label one disc "**1**", two discs "**2**", three discs "**3**", ..., fifty discs "**50**". Put these $1+2+3+\cdots+50=1275$ labeled discs in a box. Discs are then drawn from the box at random without replacement. What is the minimum number of discs that must me drawn in order to guarantee drawing at least ten discs with the same label?

95 Problem Given any set of ten natural numbers between 1 and 99 inclusive, prove that there are two disjoint nonempty subsets of the set with equal sums of their elements.

Answers

70 Either n is a perfect square, $n=a^2$ in which case $2<a<2a\le n-1$ and hence a and $2a$ are among the numbers $\{3,4,\ldots,n-1\}$ or n is not a perfect square, but still composite, with $n=ab$, $1<a<b<n-1$.

71 If $p>3$ and prime, p is odd. But then one of the three consecutive odd numbers p, $p+2$, $p+4$, must be divisible by 3 and is different from 3 and hence not a prime.

72 We have $3x+2=7a$, with a an integer. Furthermore, $15x^2-11x-14=(3x+2)(5x-7)=7a(5x-7)$, whence 7 divides $15x^2-11x-14$.

73 There are 27 different sums. The sums 1 and 27 only appear once (in 100 and 999), each of the other 25 sums appears thrice, at least. Thus if $27+25+1=53$ are drawn, at least 3 chips will have the same sum.

74 If s is itself a power of 2 then we are done. Assume that s is strictly between two powers of 2: $2^{r-1}<s<2^r$. Then $s<2^r<2s<2^{r+1}$, and so the interval $[s;2s]$ contains 2^r, a power of 2.

75 Since p and q are odd, we know that $p+q$ is even, and so $\dfrac{p+q}{2}$ is an integer. But $p<q$ gives $2p<p+q<2q$ and so $p<\dfrac{p+q}{2}<q$, that is, the average of p and q lies between them. Since p and q are consecutive primes, any number between them is composite, and so divisible by at least two primes. So $p+q=2\left(\dfrac{p+q}{2}\right)$ is divisible by the prime 2 and by at least two other primes dividing $\dfrac{p+q}{2}$.

76 The neighbors of

a			d
e			h
	n	o	

is exactly the sum of all the elements of the table. Hence the sum sought is 6.

77 We have

$$\begin{aligned} x^4+2x^2+2x+2 &= (x^2+ax+b)(x^2+cx+d)\\ &= x^4+(a+c)x^3+(d+b+ac)x^2+(ad+bc)x+bd. \end{aligned}$$

Thus

$$bd=2,\quad ad+bc=2,\quad d+b+bc=2,\quad a+c=2.$$

Assume a,b,c,d are integers. Since $bd=2$, bd must be of opposite parity (one odd, the other even). But then $d+b$ must be odd, and since $d+b+bc=2$, bc must be odd, meaning that both b and c are odd, whence d is even. Therefore ad is even, and so $ad+bc=2$ is even plus odd, that is, odd: a contradiction since 2 is not odd.

78 Let

$$P(n):\quad \underbrace{\sqrt{a+\sqrt{a+\sqrt{a+\cdots+\sqrt{a}}}}}_{n \text{ radicands}}<\frac{1+\sqrt{4a+1}}{2}.$$

Let us prove $P(1)$, that is

$$\forall a>0,\quad \sqrt{a}<\frac{1+\sqrt{4a+1}}{2}.$$

To get this one, let's work backwards. If $a>\dfrac{1}{4}$

$$\begin{aligned} \sqrt{a}<\frac{1+\sqrt{4a+1}}{2} &\iff 2\sqrt{a}<1+\sqrt{4a+1}\\ &\iff 2\sqrt{a}-1<\sqrt{4a+1}\\ &\iff (2\sqrt{a}-1)^2<(\sqrt{4a+1})^2\\ &\iff 4a-4\sqrt{a}+1<4a+1\\ &\iff -2\sqrt{a}<0. \end{aligned}$$

all the steps are reversible and the last inequality is always true. If $a \le \frac{1}{4}$ then trivially $2\sqrt{a}-1 < \sqrt{4a+1}$. Thus $P(1)$ is true. Assume now that $P(n)$ is true and let's derive $P(n+1)$. From

$$\underbrace{\sqrt{a+\sqrt{a+\sqrt{a+\cdots+\sqrt{a}}}}}_{n \text{ radicands}} < \frac{1+\sqrt{4a+1}}{2} \implies \underbrace{\sqrt{a+\sqrt{a+\sqrt{a+\cdots+\sqrt{a}}}}}_{n+1 \text{ radicands}} < \sqrt{a+\frac{1+\sqrt{4a+1}}{2}}.$$

we see that it is enough to shew that

$$\sqrt{a+\frac{1+\sqrt{4a+1}}{2}} = \frac{1+\sqrt{4a+1}}{2}.$$

But observe that

$$(\sqrt{4a+1}+1)^2 = 4a+2\sqrt{4a+1}+2 \quad \implies \quad \frac{1+\sqrt{4a+1}}{2} = \sqrt{a+\frac{1+\sqrt{4a+1}}{2}},$$

proving the claim.

79 We have

$$\sqrt[4]{abcd} = \sqrt{\sqrt{ab}\cdot\sqrt{cd}} \le \frac{\sqrt{ab}+\sqrt{cd}}{2} \le \frac{\frac{a+b}{2}+\frac{c+d}{2}}{2} = \frac{a+b+c+d}{4}.$$

Now let $a=u, b=v, c=w$ and $d=\dfrac{u+v+w}{3}$. Then

$$\begin{aligned}
\sqrt[4]{uvw\left(\frac{u+v+w}{3}\right)} \le \frac{u+v+w+\frac{u+v+w}{3}}{4} \quad &\implies \quad (uvw)^{1/4}\left(\frac{u+v+w}{3}\right)^{1/4} \le \frac{u+v+w}{3} \\
&\implies \quad (uvw)^{1/4} \le \left(\frac{u+v+w}{3}\right)^{1-1/4} \\
&\implies \quad (uvw)^{1/4} \le \left(\frac{u+v+w}{3}\right)^{3/4} \\
&\implies \quad (uvw)^{1/3} \le \frac{u+v+w}{3},
\end{aligned}$$

whence the required result follows.

80 Since squares of real numbers are non-negative, we have

$$\begin{aligned}
(a-b)^2+(b-c)^2+(c-a)^2 \ge 0 \quad &\iff \quad 2a^2+2b^2+2c^2-2ab-2bc-2ca \ge 0 \\
&\iff \quad a^2+b^2+c^2-ab-bc-ca \ge 0.
\end{aligned}$$

Now, use the identity

$$x^3+y^3 = (x+y)^3-3xy(x+y)$$

twice. Then

$$\begin{aligned}
a^3+b^3+c^3-3abc &= (a+b)^3+c^3-3ab(a+b)-3abc \\
&= (a+b+c)^3-3(a+b)c(a+b+c)-3ab(a+b+c) \\
&= (a+b+c)((a+b+c)^2-3ac-3bc-3ab) \\
&= (a+b+c)(a^2+b^2+c^2-ab-bc-ca)
\end{aligned}$$

If a,b,c are non-negative then $a+b+c \ge 0$ and also $a^2+b^2+c^2-ab-bc-ca \ge 0$. This gives

$$\frac{a^3+b^3+c^3}{3} \ge abc.$$

The desired inequality follows upon putting $u=a^3, v=b^3, w=c^3$.

81 We have

$$\begin{aligned}
(8k\pm 1)^2 &= 64k^2 \pm 16k+1 = 8(8k^2\pm 2)+1, \\
(8k\pm 3)^2 &= 64k^2 \pm 48k+9 = 8(8k^2\pm 6+1)+1,
\end{aligned}$$

proving that in all cases the remainder is 1 upon division by 8.

Now, a sum of three odd squares must leave remainder 3 upon division by 8. Thus if 2001 were a sum of three squares, it would leave remainder $3=1+1+1$ upon division by 8. But 2001 leaves remainder 1 upon division by 8, a contradiction to the assumption that it is a sum of three squares.

82 We are required to find

$$1+3+\cdots+(2n-1).$$

Observe that $1=1^2$; $1+3=2^2$; $1+3+5=3^2$; $1+3+5+7=4^2$. We suspect that

$$1+3+\cdots+(2n-1)=n^2,$$

which we will prove by induction. We have already established this for $n=1$. Let P_{n-1} be the proposition

$$1+3+\cdots+(2n-3)=(n-1)^2,$$

which we assume true. Now

$$\begin{aligned} 1+3+\cdots+(2n-1) &= 1+3+\cdots+(2n-3)+(2n-1) \\ &= (n-1)^2+2n-1 \\ &= n^2-2n+1+2n-1 \\ &= n^2, \end{aligned}$$

establishing the truth of P_n.

83 The assertion is clear for $n=1$ since a straight line divides the plane into two regions. Assume P_{n-1}, that is, that $n-1$ non-parallel straight lines intersecting at a common point divide the plane into $2(n-1)=2n-2$ regions. A new line non-parallel to them but passing through a common point will lie between two of the old lines, and divide the region between them into two more regions, producing then $2n-2+2=2n$ regions, demonstrating the assertion.

84 For $n=1$ straight lines this is clear. Assume P_{n-1}, the proposition that this is possible for $n-1>1$ lines is true. So consider the plane split by $n-1$ lines into regions and coloured as required. Consider now a new line added to the $n-1$ lines. This line splits the plane into two regions, say I and II. We now do the following: in region I we leave the original coloration. In region II we switch the colours. We now have a coloring of the plane in the desired manner. For, either the two regions lie completely in region I or completely in region II, and they are coloured in the desired manner by the induction hypothesis. If one lies in region I and the other in region II, then they are coloured in the prescribed manner because we switched the colours in the second region.

85 For $n=0$ this is the identity $\sin 2\theta = 2\sin\theta\cos\theta$. Assume the statement is true for $n-1$, that is, assume that

$$(\cos\theta)(\cos 2\theta)\cdots(\cos 2^{n-1}\theta)=\frac{\sin 2^n\theta}{2^n\sin\theta}.$$

Then

$$\begin{aligned} (\cos\theta)(\cos 2\theta)\cdots(\cos 2^n\theta) &= (\cos\theta)(\cos 2\theta)\cdots(\cos 2^{n-1}\theta)(\cos 2^n\theta) \\ &= \frac{\sin 2^n\theta}{2^n\sin\theta}(\cos 2^n\theta) \\ &= \frac{\sin 2^{n+1}\theta}{2^{n+1}\sin\theta}, \end{aligned}$$

as wanted.

86 The formula clearly holds for $n=1$. Assume that

$$\sin x+\sin 2x+\cdots+\sin(n-1)x=\frac{\sin\frac{n}{2}x}{\sin\frac{x}{2}}\cdot\sin\frac{(n-1)x}{2}.$$

Then

$$\begin{aligned} \sin x+\sin 2x+\cdots+\sin nx &= \sin x+\sin 2x+\cdots+\sin(n-1)x+\sin nx \\ &= \frac{\sin\frac{n}{2}x}{\sin\frac{x}{2}}\cdot\sin\tfrac{(n-1)x}{2}+\sin nx \\ &= \frac{\sin\frac{n}{2}x}{\sin\frac{x}{2}}\cdot\sin\tfrac{(n-1)x}{2}+2\sin\tfrac{nx}{2}\cos\tfrac{nx}{2} \\ &= \left(\frac{\sin\frac{(n-1)x}{2}+2\cos\frac{nx}{2}\sin\frac{x}{2}}{\sin\frac{x}{2}}\right)(\sin\tfrac{nx}{2}) \\ &= \left(\frac{\sin\frac{nx}{2}\cos\frac{x}{2}-\sin\frac{x}{2}\cos\frac{nx}{2}+2\cos\frac{nx}{2}\sin\frac{x}{2}}{\sin\frac{x}{2}}\right)(\sin\tfrac{nx}{2}) \\ &= \left(\frac{\sin\frac{nx}{2}\cos\frac{x}{2}+\sin\frac{x}{2}\cos\frac{nx}{2}}{\sin\frac{x}{2}}\right)(\sin\tfrac{nx}{2}) \\ &= \frac{\sin\frac{n+1}{2}x}{\sin\frac{x}{2}}\cdot\sin\tfrac{nx}{2}, \end{aligned}$$

where we have used the sum identity

$$\sin(a\pm b)=\sin a\cos b\pm\sin b\cos a.$$

87 For $n=0$ we have $2^0=1>0$, and for $n=1$ we have $2^1=2>1$ so the assertion is true when $n=0$ and $n=1$. Assume the assertion is true for $n-1>0$, that is, assume that $2^{n-1}>n-1$. Examine

$$2^n=2(2^{n-1})=2^{n-1}+2^{n-1}>n-1+n-1\geq n-1+1=n,$$

using the induction hypothesis and the fact that $n-1\geq 1$.

88 For $n=1$ we have $1\cdot 2=2+(1-1)2^2$, and so the statement is true for $n=1$. Assume the statement is true for n, that is, assume

$$P(n):1\cdot 2+2\cdot 2^2+3\cdot 2^3+\cdots+n\cdot 2^n=2+(n-1)2^{n+1}.$$

We would like to prove that we indeed have

$$P(n+1):1\cdot 2+2\cdot 2^2+3\cdot 2^3+\cdots+(n+1)\cdot 2^{n+1}=2+n2^{n+2}.$$

But adding $(n+1)2^{n+1}$ to both sides of $P(n)$ we obtain

$$1\cdot 2+2\cdot 2^2+3\cdot 2^3+\cdots+n\cdot 2^n+(n+1)2^{n+1}=2+(n-1)2^{n+1}+(n+1)2^{n+1}=2+2n2^{n+1}=2+n2^{n+2},$$

proving $P(n+1)$.

89 If all the magenta, all the yellow, all the white, 14 of the red and 14 of the blue marbles are drawn, then in among these $8+10+12+14+14=58$ there are no 15 marbles of the same color. Thus we need 59 marbles in order to insure that there will be 15 marbles of the same color.

90 There are seven possible sums, each one a number in $\{-3,-2,-1,0,1,2,3\}$. By the Pigeonhole Principle, two of the eight sums must add up to the same.

91 Pick a pair of different sex facing one another, that is, forming a "diameter" on the table. On either side of the diameter there must be an equal number of people, that is, forty nine. If all the men were on one side of the diameter then we would have a total of $49+1=50$, a contradiction.

92 We have $\lceil\!\lceil \frac{16}{5} \rceil\!\rceil = 4$, so there is at least one cat who has four kittens.

93 First observe that if we choose $n+1$ integers from any string of $2n$ consecutive integers, there will always be some two that differ by n. This is because we can pair the $2n$ consecutive integers

$$\{a+1,a+2,a+3,\ldots,a+2n\}$$

into the n pairs

$$\{a+1,a+n+1\},\{a+2,a+n+2\},\ldots,\{a+n,a+2n\},$$

and if $n+1$ integers are chosen from this, there must be two that belong to the same group.

So now group the one hundred integers as follows:

$$\{1,2,\ldots 20\},\{21,22,\ldots,40\},$$

$$\{41,42,\ldots,60\},\ \{61,62,\ldots,80\}$$

and

$$\{81,82,\ldots,100\}.$$

If we select fifty five integers, we must perforce choose eleven from some group. From that group, by the above observation (let $n=10$), there must be two that differ by 10.

94 If we draw all the $1+2+\cdots+9=45$ labelled "**1**", ..., "**9**" and any nine from each of the discs "**10**", ..., "**50**", we have drawn $45+9\cdot 41=414$ discs. The 415-th disc drawn will assure at least ten discs from a label.

95 There are $2^{10}-1=1023$ non-empty subsets that one can form with a given 10-element set. To each of these subsets we associate the sum of its elements. The maximum value that any such sum can achieve is $90+91+\cdots+99=945<1023$. Therefore, there must be at least two different subsets that have the same sum.

Chapter 3

Logic, Sets, and Boolean Algebra

3.1 Logic

96 Definition A *boolean proposition* is a statement which can be characterised as either **true** or **false** .

Whether the statement is *obviously* true or false does not enter in the definition. One only needs to know that its certainty can be established.

97 Example The following are boolean propositions and their values, if known:

1. $7^2 = 49$. (**true**)
2. $5 > 6$. (**false**)
3. If p is a prime then p is odd. (**false**)
4. There exists infinitely many primes which are the sum of a square and 1. (unknown)
5. There is a G-d. (unknown)
6. There is a dog. (**true**)
7. I am the Pope. (**false**)
8. Every prime that leaves remainder 1 when divided by 4 is the sum of two squares. (**true**)
9. Every even integer greater than 6 is the sum of two distinct primes. (unknown)

98 Example The following are not boolean propositions, since it is impossible to assign a **true** or **false** value to them.

1. Whenever I shampoo my camel.
2. Sit on a potato pan, Otis!
3. $y \leftarrow x$.
4. This sentence is false.

99 Definition A *boolean operator* is a character used on boolean propositions. Its output is either **true** or **false**

We will consider the following boolean operators in these notes. They are listed in order of operator precedence and their evaluation rules are given in Table **??**.

1. $\neg$ (**not** or negation),
2. $\wedge$ (**and** or conjunction)
3. $\vee$ (**or** or disjunction)
4. $\Longrightarrow$ (**implies**)
5. $=$ (**equals**)

$\neg$ has right-to-left associativity, all other operators listed have left-to-right associativity.

*The $\vee =$ **or** is inclusive, meaning that if $a \vee b$ then either a is true, or b is true, or both a and b are true.*

a	b	$(\neg a)$	$(a \wedge b)$	$(a \vee b)$	$(a \implies b)$	$(a = b)$
F	F	T	F	F	T	T
F	T	T	F	T	T	F
T	F	F	F	T	F	F
T	T	F	T	T	T	T

Table 3.1: Evaluation Rules

100 Example Consider the propositions:

- a : I will eat my socks.
- b : It is snowing.
- c : I will go jogging.

The sentences below are represented by means of logical operators.

❶ $(b \vee \neg b) \implies c$: Whether or not it is snowing, I will go jogging.

❷ $b \implies \neg c$: If it is snowing, I will not go jogging.

❸ $b \implies (a \wedge \neg c)$: If it is snowing, I will eat my socks, but I will not go jogging.

101 Example $\neg a \implies a \vee b$ is equivalent to $(\neg a) \implies (a \vee b)$ upon using the precedence rules.

102 Example $a \implies b \implies c$ is equivalent to $(a \implies b) \implies c$ upon using the associativity rules.

103 Example $a \wedge \neg b \implies c$ is equivalent to $(a \wedge \neg b) \implies c$ by the precedence rules.

104 Example Write a code fragment that accepts three numbers, decides whether they form the sides of a triangle.

Solution: First we must have $a > 0, b > 0, c > 0$. Sides of length a, b, c form a triangle if and only they satisfy the triangle inequalities::

$$a + b > c,$$

$$b + c > a,$$

$$c + a > b.$$

Algorithm 3.1.1: ISITATRIANGLE$((a,b,c))$

if $((a > 0)$ **and** $(b > 0)$ **and** $(c > 0)$
and $((a + b > c)$ **and** $(b + c > a)$ **and** $(c + a > b))$
then istriangle $\leftarrow$ **true**
else istriangle $\leftarrow$ **false**
return (istriangle)

105 Definition A *truth table* is a table assigning all possible combinations of T or F to the variables in a proposition. If there are n variables, the truth table will have 2^n lines.

106 Example Construct the truth table of the proposition $a \vee \neg b \wedge c$.

Solution: Since there are three variables, the truth table will have $2^3 = 8$ lines. Notice that by the precedence rules the given proposition is equivalent to $a \vee (\neg b \wedge c)$, since $\wedge$ has higher precedence than $\vee$. The truth table is in Table **??**.

107 Definition Two propositions are said to be *equivalent* if they have the same truth table. If proposition P is equivalent to proposition Q we write $P = Q$.

a	b	c	$(\neg b)$	$(\neg b \wedge c)$	$a \vee (\neg b \wedge c)$
F	F	F	T	F	F
F	F	T	T	T	T
F	T	F	F	F	F
F	T	T	F	F	F
T	F	F	T	F	T
T	F	T	T	T	T
T	T	F	F	F	T
T	T	T	F	F	T

Table 3.2: Example **??**.

a	$(\neg a)$	$(\neg(\neg a))$
F	T	F
T	F	T

Table 3.3: Theorem **??**.

108 Theorem (Double Negation) $\neg(\neg a) = a$.

Proof: *From the truth table* **??** *the entries for a and* $\neg(\neg a)$ *produce the same output, proving the assertion.* ❑

109 Theorem (De Morgan's Rules) $\neg(a \vee b) = \neg a \wedge \neg b$ and $\neg(a \wedge b) = \neg a \vee \neg b$.

Proof: *Truth table* **??** *proves that* $\neg(a \vee b) = \neg a \wedge \neg b$ *and truth table* **??** *proves that* $\neg(a \wedge b) = \neg a \vee \neg b$.

a	b	$(a \vee b)$	$\neg(a \vee b)$	$(\neg a)$	$(\neg b)$	$(\neg a \wedge \neg b)$
F	F	F	T	T	T	T
F	T	T	F	T	F	F
T	F	T	F	F	T	F
T	T	T	F	F	F	F

Table 3.4: $\neg(a \vee b) = \neg a \wedge \neg b$.

a	b	$(a \wedge b)$	$\neg(a \wedge b)$	$(\neg a)$	$(\neg b)$	$(\neg a \vee \neg b)$
F	F	F	T	T	T	T
F	T	F	T	T	F	T
T	F	F	T	F	T	T
T	T	T	F	F	F	F

Table 3.5: $\neg(a \wedge b) = \neg a \vee \neg b$.

❑

110 Example Negate $A \vee \neg B$.

Solution: Using the De Morgan Rules and double negation: $\neg(A \vee \neg B) = \neg A \wedge \neg(\neg B) = \neg A \wedge B$.

111 Example Let p and q be propositions. Translate into symbols: either p or q is true, but not both simultaneously.

Solution: By the conditions of the problem, if p is true then q must be false, which we represent as $p \wedge \neg q$. Similarly if q is true, p must be false and we must have $\neg p \wedge q$. The required expression is thus

$$(p \wedge \neg q) \vee (\neg p \wedge q).$$

112 Definition A *predicate* is a sentence containing variables, whose truth or falsity depends on the values assigned to the variables.

113 Definition (Existential Quantifier) We use the symbol $\exists$ to mean "there exists."

114 Definition (Universal Quantifier) We use the symbol $\forall$ to mean "for all."

Observe that $\neg\forall = \exists$ and $\neg\exists = \forall$.

115 Example Write the negation of $(\forall n \in \mathbb{N})(\exists x \in]0;+\infty[)(nx < 1)$.

Solution: Since $\neg(\forall n \in \mathbb{N}) = (\exists n \in \mathbb{N})$, $\neg(\exists x \in]0;+\infty[) = (\forall x \in]0;+\infty[)$ and $\neg(nx < 1) = (nx \geq 1)$, the required statement is

$$(\exists n \in \mathbb{N})(\forall x \in]0;+\infty[)(nx \geq 1).$$

3.2 Sets

We will consider a *set* naively as a collection of objects called *elements*. We use the boldface letters $\mathbb{N}$ to denote the natural numbers (non-negative integers) and $\mathbb{Z}$ to denote the integers. The boldface letters $\mathbb{R}$ and $\mathbb{C}$ shall respectively denote the real numbers and the complex numbers.

If S is a set and the element x is in the set, then we say that x *belongs to* S and we write this as $x \in S$. If x does not belong to S we write $x \notin S$. For example if $S = \{n \in \mathbb{N} : n \text{ is the square of an integer }\}$, then $4 \in S$ but $2 \notin S$. We denote by $\text{card}\,(A)$ the *cardinality* of A, that is, the number of elements that A has.

If a set A is totally contained in another set B, then we say that A *is a subset of* B and we write this as $A \subseteq B$ (some authors use the notation $A \subset B$). For example, if $S = \{\text{squares of integers}\}$, then $A = \{1,4,9,16\}$ is a subset of S. If $\exists x \in A$ such that $x \notin B$, then A is not a subset of B, which we write as $A \not\subseteq B$. Two sets A and B are equal if $A \subseteq B$ and $B \subseteq A$.

116 Example Find all the subsets of $\{a,b,c\}$.

Solution: They are

$$\begin{array}{rcl} S_1 &=& \varnothing \\ S_2 &=& \{a\} \\ S_3 &=& \{b\} \\ S_4 &=& \{c\} \\ S_5 &=& \{a,b\} \\ S_6 &=& \{b,c\} \\ S_7 &=& \{c,a\} \\ S_8 &=& \{a,b,c\} \end{array}$$

117 Example Find all the subsets of $\{a,b,c,d\}$.

Solution: The idea is the following. We use the result of example **??**. Now, a subset of $\{a,b,c,d\}$ either contains d or it does not. Since the subsets of $\{a,b,c\}$ do not contain d, we simply list all the subsets of $\{a,b,c\}$ and then to each one of them we add d. This gives

$$\begin{array}{rcl} S_1 &=& \varnothing \\ S_2 &=& \{a\} \\ S_3 &=& \{b\} \\ S_4 &=& \{c\} \\ S_5 &=& \{a,b\} \\ S_6 &=& \{b,c\} \\ S_7 &=& \{c,a\} \\ S_8 &=& \{a,b,c\} \end{array} \qquad \begin{array}{rcl} S_9 &=& \{d\} \\ S_{10} &=& \{a,d\} \\ S_{11} &=& \{b,d\} \\ S_{12} &=& \{c,d\} \\ S_{13} &=& \{a,b,d\} \\ S_{14} &=& \{b,c,d\} \\ S_{15} &=& \{c,a,d\} \\ S_{16} &=& \{a,b,c,d\} \end{array}$$

118 Theorem A finite n-element set has 2^n subsets.

Proof: *We use induction and the idea of example* **??**. *Clearly a set A with $n = 1$ elements has $2^1 = 2$ subsets: $\varnothing$ and A itself. Assume every set with $n-1$ elements has 2^{n-1} subsets. Let B be a set with n elements. If $x \in B$ then $B \setminus \{x\}$ is a set with $n-1$ elements and so by the induction hypothesis it has 2^{n-1} subsets. For each subset $S \subseteq B \setminus \{x\}$ we form the new subset $S \cup \{x\}$. This is a subset of B. There are 2^{n-1} such new subsets, and so B has a total of $2^{n-1} + 2^{n-1} = 2^n$ subsets.* ❑

119 Definition The *union* of two sets A and B, is the set

$$A \cup B = \{x : (x \in A) \vee (x \in B)\}.$$

This is read "A union B." See figure **??**. The *intersection* of two sets A and B, is

$$A \cap B = \{x : (x \in A) \ \wedge \ (x \in B)\}.$$

This is read "A intersection B." See figure **??**. The *difference* of two sets A and B, is

$$A \setminus B = \{x : (x \in A) \ \wedge (x \notin B)\}.$$

This is read "A set minus B." See figure **??**.

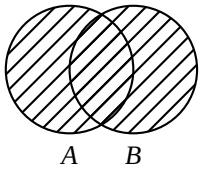

Figure 3.1: $A \cup B$

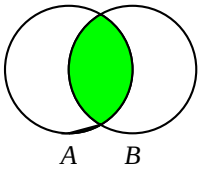

Figure 3.2: $A \cap B$

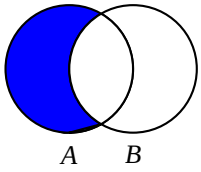

Figure 3.3: $A \setminus B$

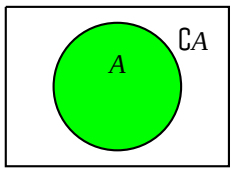

Figure 3.4: $\complement A$

120 Definition Let $A \subseteq X$. The *complement* of A with respect to X is $\complement A = X \setminus A$.

Observe that $\complement A$ is all that which is outside A. Usually we assume that A is a subset of some universal set U which is tacitly understood. The complement $\complement A$ represents the event that A does not occur. We represent $\complement A$ pictorially as in figure **??**.

121 Example Let $U = \{0,1,2,3,4,5,6,7,8,9\}$ be the universal set of the decimal digits and let $A = \{0,2,4,6,8\} \subset U$ be the set of even digits. Then $\complement A = \{1,3,5,7,9\}$ is the set of odd digits.

Observe that

$$\complement A \cap A = \varnothing. \tag{3.1}$$

We also have the *De Morgan Laws*: if A and B share the same universal set, we have

$$\complement(A \cup B) = \complement A \cap \complement B, \tag{3.2}$$

$$\complement(A \cap B) = \complement A \cup \complement B. \tag{3.3}$$

We will now prove one of the De Morgan's Rules.

122 Example Prove that $\complement(A \cup B) = \complement A \cap \complement B$.

Solution: Let $x \in \complement(A \cup B)$. Then $x \notin A \cup B$. Thus $x \notin A \wedge x \notin B$, that is, $x \in \complement A \wedge x \in \complement B$. This is the same as $x \in \complement A \cap \complement B$. Therefore $\complement(A \cup B) \subseteq \complement A \cap \complement B$.

Now, let $x \in \complement A \cap \complement B$. Then $x \in \complement A \wedge x \in \complement B$. This means that $x \notin A \wedge x \notin B$ or what is the same $x \notin A \cup B$. But this last statement asserts that $x \in \complement(A \cup B)$. Hence $\complement A \cap \complement B \subseteq \complement(A \cup B)$.

Since we have shown that the two sets contain each other, it must be the case that they are equal.

123 Example Prove that $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.

Solution: We have

$$\begin{array}{rcl} x \in A \setminus (B \cup C) & \iff & x \in A \wedge x \notin (B \vee C) \\ & \iff & (x \in A) \ \wedge \ ((x \notin B) \ \wedge \ (x \notin C)) \\ & \iff & (x \in A \ \wedge \ x \notin B) \ \wedge \ (x \in A \ \wedge \ x \notin C) \\ & \iff & (x \in A \setminus B) \ \wedge \ (x \in A \setminus C) \\ & \iff & x \in (A \setminus B) \cap (A \setminus C) \end{array}$$

124 Example Shew how to write the union $A \cup B \cup C$ as a *disjoint* union of sets.

Solution: The sets $A, B \setminus A, C \setminus (A \cup B)$ are clearly disjoint and

$$A \cup B \cup C = A \cup (B \setminus A) \cup (C \setminus (A \cup B)).$$

125 Example Let $x_1 < x_2 < \cdots < x_n$ and $y_1 < y_2 < \cdots < y_m$ be two strictly increasing sequences of integers. Write an algorithm to determine

$$\{x_1, x_2, \ldots, x_n\} \cap \{y_1, y_2, \ldots, y_m\}.$$

Solution:

Algorithm 3.2.1: INTERSECTION(n, m, X, Y)

comment: X is an array of length n.

comment: Y is an array of length m.

$n1 \leftarrow 0$
$m1 \leftarrow 0$
common $\leftarrow 0$
while $(n1 \neq n)$ **and** $(m1 \neq m)$
do
- **if** $X[n1+1] < Y[m1+1]$
  - **then** $n1 \leftarrow n1+1$
  - **else if** $X[n1+1] > Y[m1+1]$
  - **then** $m1 \leftarrow m1+1$
  - **else**
    - $n1 \leftarrow n1+1$
    - $m1 \leftarrow m1+1$
    - common $\leftarrow$ common $+1$

3.3 Boolean Algebras and Boolean Operations

126 Definition A *boolean algebra* consists of a set X with at least two different elements 0 and 1, two binary operations $+$ (addition) and $\cdot$ (multiplication), and a unary operation $\overline{}$ (called *complementation*) satisfying the following axioms. (We use the juxtaposition AB to denote the product $A \cdot B$.)

1. $A+B = B+A$ (commutativity of addition)
2. $AB = BA$ (commutativity of multiplication)
3. $A+(B+C) = (A+B)+C$ (associativity of addition)
4. $A(BC) = (AB)C$ (associativity of multiplication)
5. $A(B+C) = AB+AC$ (distributive law)
6. $A+(BC) = (A+B)(A+C)$ (distributive law)
7. $A+0 = A$ (0 is the additive identity)
8. $A1 = A$ (1 is the multiplicative identity)
9. $A+\overline{A} = 1$
10. $A\overline{A} = 0$

127 Example If we regard $0 = F$, $1 = T$, $+ = \vee$, $\cdot = \wedge$, and $\overline{} = \neg$, then the logic operations over $\{F, T\}$ constitute a boolean algebra.

128 Example If we regard $0 = \varnothing$, $1 = U$ (the universal set), $+ = \cup$, $\cdot = \cap$, and $\overline{} = \complement$, then the set operations over the subsets of U constitute a boolean algebra.

129 Example Let $X = \{1, 2, 3, 5, 6, 10, 15, 30\}$, the set of positive divisors of 30. We define $+$ as the least common multiple of two elements, $\cdot$ as the greatest common divisor of two elements, and $\overline{A} = \dfrac{30}{A}$. The additive identity is 1 and the multiplicative identity is 30. Under these operations X becomes a boolean algebra.

A	B	$\overline{A}$	$A+B$	AB
0	0	1	0	0
0	1	1	1	0
1	0	0	1	0
1	1	0	1	1

Table 3.6: Evaluation Rules

The operations of complementation, addition and multiplication act on 0 and 1 as shewn in table **??**.
The following properties are immediate.

130 Theorem $\overline{0}=1$ and $\overline{1}=0$.

Proof: *Since* 0 *is the additive identity,* $\overline{0}=\overline{0}+0$. *But by axiom* **??**, $\overline{0}+0=1$ *and thus* $\overline{0}=\overline{0}+0=1$.

Similarly, since 1 *is the multiplicative identity,* $\overline{1}=1\cdot\overline{1}$. *But by axiom* **??**, $1\cdot\overline{1}=0$ *and thus* $\overline{1}=1\cdot\overline{1}=0$. ❑

131 Theorem (Idempotent Laws) $A+A=A$ and $AA=A$

Proof: *We have*

$$A=A+0=A+A\cdot\overline{A}=(A+A)(A+\overline{A})=(A+A)(1)=A+A.$$

Similarly

$$A=A1=A(A+\overline{A})=AA+A\cdot\overline{A}=AA+0=AA.$$

❑

132 Theorem (Domination Laws) $A+1=1$ and $A\cdot 0=0$.

Proof: *We have*

$$A+1=A+(A+\overline{A})=(A+A)+\overline{A}=A+\overline{A}=1.$$

Also,

$$A\cdot 0=A(A\cdot\overline{A})=(AA)\overline{A}=A\overline{A}=0.$$

❑

133 Theorem (Uniqueness of the Complement) If $AB=0$ and $A+B=1$ then $B=\overline{A}$.

Proof: *We have*

$$B=B1=B(A+\overline{A})=BA+B\overline{A}=0+B\overline{A}=B\overline{A}.$$

Also,

$$\overline{A}=\overline{A}1=\overline{A}(A+B)=\overline{A}\cdot A+\overline{A}B=\overline{A}B.$$

Thus

$$B=B\overline{A}=\overline{A}B=\overline{A}.$$

❑

134 Theorem (Involution Law) $\overline{\overline{A}}=A$

Proof: *By axioms* **??** *and* **??**, *we have the identities*

$$1=\overline{A}+\overline{\overline{A}} \text{ and } \overline{\overline{A}}\cdot\overline{A}=0.$$

By uniqueness of the complement we must have $A=\overline{\overline{A}}$. ❑

135 Theorem (De Morgan's Laws) $\overline{A+B}=\overline{A}\cdot\overline{B}$ and $\overline{A\cdot B}=\overline{A}+\overline{B}$.

Proof: *Observe that*

$$(A+B)+\overline{A}\cdot\overline{B}=(A+B+\overline{A})(A+B+\overline{B})=(B+1)(A+1)=1,$$

and

$$(A+B)\overline{A}\cdot\overline{B}=A\overline{A}\cdot\overline{B}+B\overline{A}\cdot\overline{B}=0+0=0.$$

Thus $\overline{A}\cdot\overline{B}$ *is the complement of* $A+B$ *and so we must have* $\overline{A}\cdot\overline{B}=\overline{A+B}$.

To obtain the other De Morgan Law put $\overline{A}$ *instead of A and* $\overline{B}$ *instead of B in the law just derived and use the involution law:*

$$\overline{\overline{A}+\overline{B}}=\overline{\overline{A}}\cdot\overline{\overline{B}}=AB.$$

Taking complements once again we have

$$\overline{\overline{A}+\overline{B}}=AB\implies\overline{A}+\overline{B}=\overline{AB}.$$

❑

136 Theorem $AB+A\overline{B}=A$.

Proof: *Factoring*

$$AB+A\overline{B}=A(B+\overline{B})=A(1)=A.$$

❑

137 Theorem $A(\overline{A}+B)=AB$ and $A+\overline{A}B=A+B$.

Proof: *Multiplying*

$$A(\overline{A}+B)=A\overline{A}+AB=0+AB=AB.$$

Using the distributive law,

$$A+\overline{A}B=(A+\overline{A})(A+B)=1(A+B)=A+B.$$

❑

138 Theorem (Absorption Laws) $A+AB=A$ and $A(A+B)=A$.

Proof: *Factoring and using the domination laws:*

$$A+AB=A(1+B)=A1=A.$$

Expanding and using the identity just derived:

$$A(A+B)=AA+AB=A+AB=A.$$

❑

3.4 Sum of Products and Products of Sums

Given a truth table in some boolean variables, we would like to find a function whose output is that of the table. This can be done by either finding a *sum of products* (SOP) or a *product of sums* (POS) for the table. To find a sum of products from a truth table:

❶ identify the rows having output 1.

❷ for each such row, write the variable if the variable input is 1 or write the complement of the variable if the variable input is 0, then multiply the variables forming a term.

❸ add all such terms.

To find a product of sums from a truth table:

❶ identify the rows having output 0.

❷ for each such row, write the variable if the variable input is 0 or write the complement of the variable if the variable input is 1, then add the variables forming a sum

❸ multiply all such sums.

139 Example Find a SOP and a POS for Z.

A	B	C	Z
0	0	0	1
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	1

Solution: The output (Z) 1's occur on the rows (i) $A=0,B=0,C=0$, so we form the term $(\overline{A})(\overline{B})(\overline{C})$, (ii) $A=0,B=1,C=0$, so we form the term $\overline{A}B\overline{C}$, (iii) $A=1,B=1,C=0$, so we form the term $AB\overline{C}$, and (iv) $A=B=C=1$, giving the term ABC. The required SOP is

$$Z=(\overline{A})(\overline{B})(\overline{C})+\overline{A}B\overline{C}+AB\overline{C}+ABC.$$

The output (Z) 0's occur on the rows (i) $A=0,B=0,C=1$, so we form the term $A+B+\overline{C}$, (ii) $A=0,B=1,C=1$, so we form the term $A+\overline{B}+\overline{C}$, (iii) $A=1,B=0,C=0$, so we form the term $\overline{A}+B+C$, and (iv) $A=1,B=0,C=1$, giving the term $\overline{A}+B+\overline{C}$. The required POS is

$$Z=(A+B+\overline{C})(A+\overline{B}+\overline{C})(\overline{A}+B+C)(\overline{A}+B+\overline{C}).$$

Using the axioms of a boolean algebra and the aforementioned theorems we may simplify a given boolean expression, or transform a SOP into a POS or viceversa.

140 Example Convert the following POS to a SOP:

$$(A+\overline{B}C)(A+\overline{B}D).$$

Solution:

$$\begin{aligned}(A+\overline{B}C)(A+\overline{B}D) &= AA+A\overline{B}D+A\overline{B}C+\overline{B}C\overline{B}D\\ &= A+A\overline{B}D+A\overline{B}C+\overline{B}CD\\ &= A+\overline{B}CD.\end{aligned}$$

141 Example Convert the following SOP to a POS:

$$A\overline{B}+\overline{C}D.$$

Solution:

$$\begin{aligned}A\overline{B}+\overline{C}D &= (A\overline{B}+\overline{C})(A\overline{B}+D)\\ &= (A+\overline{C})(\overline{B}+\overline{C})(A+D)(\overline{B}+D).\end{aligned}$$

142 Example Write $\overline{W}XY+\overline{W}XZ+\overline{Y+Z}$ as a sum of two products.

Solution: We have

$$\begin{aligned}\overline{W}XY+\overline{W}XZ+\overline{Y+Z} &= \overline{W}X(Y+Z)+\overline{Y+Z}\\ &= \overline{W}X+\overline{Y+Z}\\ &= \overline{W}X+\overline{Y}\cdot\overline{Z},\end{aligned}$$

where we have used the fact that $AB+\overline{B}=A+\overline{B}$ and the De Morgan laws.

3.5 Logic Puzzles

The boolean algebra identities from the preceding section may help to solve some logic puzzles.

143 Example Brown, Johns and Landau are charged with bank robbery. The thieves escaped in a car that was waiting for them. At the inquest Brown stated that the criminals had escaped in a blue Buick; Johns stated that it had been a black Chevrolet, and Landau said that it had been a Ford Granada and by no means blue. It turned out that wishing to confuse the Court, each one of them only indicated correctly either the make of the car or only its colour. What colour was the car and of what make?

Solution: Consider the sentences

A = the car is blue
B = the car is a Buick
C = the car is black
D = the car is a Chevrolet
E = the car is a Ford Granada

Since each of the criminals gave one correct answer, it follows that Brown's declaration $A+B$ is true. Similarly, Johns's declaration $C+D$ is true, and Landau's declaration $\overline{A}+E$ is true. It now follows that

$$(A+B)\cdot(C+D)\cdot(\overline{A}+E)$$

is true. Upon multiplying this out, we obtain

$$(A\cdot C\cdot\overline{A})+(A\cdot C\cdot E)+(A\cdot D\cdot\overline{A})+(A\cdot D\cdot E)+(B\cdot C\cdot\overline{A})+(B\cdot C\cdot E)+(B\cdot D\cdot\overline{A})+(B\cdot D\cdot E).$$

From the hypothesis that each of the criminals gave one correct answer, it follows that each of the summands, except the fifth, is false. Thus $B\cdot C\cdot\overline{A}$ is true, and so the criminals escaped in a black Buick.

144 Example Margie, Mimi, April, and Rachel ran a race. Asked how they made out, they replied:
Margie: "April won; Mimi was second."
Mimi: "April was second and Rachel was third."
April: "Rachel was last; Margie was second."

If each of the girls made one and only one true statement, who won the race?

Solution: Consider the sentences

A = April was first
B = April was second
C = Mimi was second
D = Margie was second
E = Rachel was third
F = Rachel was last

Since each of the girls gave one true statement we have that

$$(A+C)(B+E)(F+D)=1.$$

Multiplying this out

$$ABF+ABD+AEF+AED+CBF+CBD+CEF+CED=1.$$

Now, $AB=EF=BC=CD=0$ so the only surviving term is AED and so April was first, Margie was second, Rachel was third, and Mimi was last.

145 Example Having returned home, Maigret rang his office on quai des Orfèvres.

"Maigret here . Any news?"

"Yes Chief. The inspectors have reported. Torrence thinks that if François was drunk, then either Etienne is the murderer or François is lying. Justin is of the opinion that either Etienne is the murderer or François was not drunk and the murder occurred after midnight. Inspector Lucas asked me to tell you that if the murder had occurred after midnight, then either Etienne is the murderer or François is lying. Then there was a ring from . . . ."

"That's all, thanks. That's enough!" The commissar replaced the receiver. He knew that when François was sober he never lied. Now everything was clear to him. Find, with proof, the murderer.

Solution: Represent the following sentences as:

A = François was drunk,
B = Etienne is the murderer,
C = François is telling a lie,
D = the murder took place after midnight.

We then have

$$A \implies (B+C),\ B+\overline{A}D,\ D \implies (B+C).$$

Using the identity

$$X \implies Y = \overline{X}+Y,$$

we see that the output of the product of the following sentences must be 1:

$$(\overline{A}+B+C)(B+\overline{A}D)(\overline{D}+B+C).$$

After multiplying the above product and simplifying, we obtain

$$B+C\overline{A}D.$$

So, either Etienne is the murderer, or the following events occurred simultaneously: François lied, François was not drunk and the murder took place after midnight. But Maigret knows that $\overline{A}C = 0$, thus it follows that $E = 1$, i.e., Etienne is the murderer.

Homework

146 Problem Construct the truth table for $(p \implies q) \wedge q$.

147 Problem By means of a truth table, decide whether $(p \wedge q) \vee (\neg p) = p \vee (\neg p)$. That is, you want to compare the outputs of $(p \wedge q) \vee (\neg p)$ and $p \vee (\neg p)$.

148 Problem Explain whether the following assertion is true and negate it without using the negation symbol $\neg$:

$$\forall n \in \mathbb{N}\ \exists m \in \mathbb{N}\ \left(n > 3 \implies (n+7)^2 > 49+m\right)$$

149 Problem Explain whether the following assertion is true and negate it without using the negation symbol $\neg$:

$$\forall n \in \mathbb{N}\ \exists m \in \mathbb{N}\ \left(n^2 > 4n \implies 2^n > 2^m + 10\right)$$

150 Problem Prove by means of set inclusion that $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$.

151 Problem Obtain a sum of products for the truth table

A	B	C	Z
0	0	0	1
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	0

152 Problem Use the Inclusion-Exclusion Principle to determine how many integers in the set $\{1,2,\ldots,200\}$ are neither divisible by 3 nor 7 but are divisible by 11.

Answers

146

p	q	$p \implies q$	$(p \implies q) \wedge q$
F	F	T	F
F	T	T	T
T	F	F	F
T	T	T	T

147 The desired truth table is

p	q	$p \wedge q$	$\neg p$	$p \vee \neg p$	$(p \wedge q) \vee (\neg p)$
F	F	F	T	T	T
F	T	F	T	T	T
T	F	F	F	T	F
T	T	T	F	T	T

148 The assertion is true. We have

$$(n+7)^2 > 49+m \iff n^2+14n > m.$$

Hence, taking $m = n^2+14n-1$ for instance (or any smaller number), will make the assertion true.

150 We have,

$$\begin{aligned} x \in (A \cup B) \cap C &\iff x \in (A \cup B) \wedge x \in C \\ &\iff (x \in A \vee x \in B) \wedge x \in C \\ &\iff (x \in A \wedge x \in C) \vee (x \in B \wedge x \in C) \\ &\iff (x \in A \cap C) \vee (x \in B \cap C) \\ &\iff x \in (A \cap C) \cup (B \cap C), \end{aligned}$$

which establishes the equality.

151

$$\overline{A} \cdot \overline{B} \cdot \overline{C} + \overline{A} \cdot \overline{B} \cdot C + \overline{A} \cdot B \cdot \overline{C} + A \cdot \overline{B} \cdot \overline{C}$$

152 10

Chapter 4

Relations and Functions

4.1 Partitions and Equivalence Relations

153 Definition Let $\mathscr{S} \neq \varnothing$ be a set. A *partition* of $\mathscr{S}$ is a collection of non-empty, pairwise disjoint subsets of $\mathscr{S}$ whose union is $\mathscr{S}$.

154 Example Let

$$2\mathbb{Z} = \{\ldots,-6,-4,-2,0,2,4,6,\ldots\} = \overline{0}$$

be the set of even integers and let

$$2\mathbb{Z}+1 = \{\ldots,-5,-3,-1,1,3,5,\ldots\} = \overline{1}$$

be the set of odd integers. Then

$$(2\mathbb{Z}) \cup (2\mathbb{Z}+1) = \mathbb{Z}, \;\; (2\mathbb{Z}) \cap (2\mathbb{Z}+1) = \varnothing,$$

and so $\{2\mathbb{Z}, 2\mathbb{Z}+1\}$ is a partition of $\mathbb{Z}$.

155 Example Let

$$3\mathbb{Z} = \{\ldots -9,,-6,-3,0,3,6,9,\ldots\} = \overline{0}$$

be the integral multiples of 3, let

$$3\mathbb{Z}+1 = \{\ldots,-8,-5,-2,1,4,7,\ldots\} = \overline{1}$$

be the integers leaving remainder 1 upon division by 3, and let

$$3\mathbb{Z}+2 = \{\ldots,-7,-4,-1,2,5,8,\ldots\} = \overline{2}$$

be integers leaving remainder 2 upon division by 3. Then

$$(3\mathbb{Z}) \cup (3\mathbb{Z}+1) \cup (3\mathbb{Z}+2) = \mathbb{Z},$$
$$(3\mathbb{Z}) \cap (3\mathbb{Z}+1) = \varnothing, \; (3\mathbb{Z}) \cap (3\mathbb{Z}+2) = \varnothing, (3\mathbb{Z}+1) \cap (3\mathbb{Z}+2) = \varnothing,$$

and so $\{3\mathbb{Z}, 3\mathbb{Z}+1, 3\mathbb{Z}+2\}$ is a partition of $\mathbb{Z}$.

☞ *Notice that* $\overline{0}$ *and* $\overline{1}$ *do not mean the same in examples* **??** *and* **??**. *Whenever we make use of this notation, the integral divisor must be made explicit.*

156 Example Observe

$$\mathbb{R} = (\mathbb{Q}) \cup (\mathbb{R} \setminus \mathbb{Q}), \;\; \varnothing = (\mathbb{Q}) \cap (\mathbb{R} \setminus \mathbb{Q}),$$

which means that the real numbers can be partitioned into the rational and irrational numbers.

157 Definition Let A, B be sets. A *relation* R is a subset of the Cartesian product $A \times B$. We write the fact that $(x,y) \in R$ as $x \sim y$.

158 Definition Let A be a set and R be a relation on $A \times A$. Then R is said to be

- **reflexive** if $(\forall x \in A), x \sim x$,
- **symmetric** if $(\forall (x,y) \in A^2), x \sim y \implies y \sim x$,

- **anti-symmetric** if $(\forall (x,y) \in A^2), (x \sim y)$ **and** $(y \sim x) \implies x = y$,
- **transitive** if $(\forall (x,y,z) \in A^3), (x \sim y)$ **and** $(y \sim z) \implies (x \sim z)$.

A relation R which is reflexive, symmetric and transitive is called an *equivalence relation* on A. A relation R which is reflexive, anti-symmetric and transitive is called a *partial order* on A.

159 Example Let $\mathscr{S} = \{\text{All Human Beings}\}$, and define $\sim$ on $\mathscr{S}$ as $a \sim b$ if and only if a and b have the same mother. Then $a \sim a$ since any human a has the same mother as himself. Similarly, $a \sim b \implies b \sim a$ and $(a \sim b)$ **and** $(b \sim c) \implies (a \sim c)$. Therefore $\sim$ is an equivalence relation.

160 Example Let L be the set of all lines on the plane and write $l_1 \sim l_2$ if $l_1 || l_2$ (the line l_1 is parallel to the line l_2). Then $\sim$ is an equivalence relation on L.

161 Example Let X be a collection of sets. Write $A \sim B$ if $A \subseteq B$. Then $\sim$ is a partial order on X.

162 Example For $(a,b) \in \mathbb{R}^2$ define

$$a \sim b \Leftrightarrow a^2 + b^2 > 2.$$

Determine, with proof, whether $\sim$ is reflexive, symmetric, and/or transitive. Is $\sim$ an equivalence relation?

Solution: Since $0^2 + 0^2 \not> 2$, we have $0 \nsim 0$ and so $\sim$ is not reflexive. Now,

$$\begin{array}{rcl} a \sim b & \Leftrightarrow & a^2 + b^2 \\ & \Leftrightarrow & b^2 + a^2 \\ & \Leftrightarrow & b \sim a, \end{array}$$

so $\sim$ is symmetric. Also $0 \sim 3$ since $0^2 + 3^2 > 2$ and $3 \sim 1$ since $3^2 + 1^2 > 2$. But $0 \nsim 1$ since $0^2 + 1^2 \not> 2$. Thus the relation is not transitive. The relation, therefore, is not an equivalence relation.

163 Example For $(a,b) \in (\mathbb{Q}^*)^2$ define the relation $\sim$ as follows: $a \sim b \Leftrightarrow \frac{a}{b} \in \mathbb{Z}$. Determine whether this relation is reflexive, symmetric, and/or transitive.

Solution: $a \sim a$ since $\frac{a}{a} = 1 \in \mathbb{Z}$, and so the relation is reflexive. The relation is not symmetric. For $2 \sim 1$ since $\frac{2}{1} \in \mathbb{Z}$ but $1 \nsim 2$ since $\frac{1}{2} \notin \mathbb{Z}$. The relation is transitive. For assume $a \sim b$ and $b \sim c$. Then there exist $(m,n) \in \mathbb{Z}^2$ such that $\frac{a}{b} = m, \frac{b}{c} = n$. This gives

$$\frac{a}{c} = \frac{a}{b} \cdot \frac{b}{c} = mn \in \mathbb{Z},$$

and so $a \sim c$.

164 Example Give an example of a relation on $\mathbb{Z}^*$ which is reflexive, but is neither symmetric nor transitive.

Solution: Here is one possible example: put $a \sim b \Leftrightarrow \frac{a^2+a}{b} \in \mathbb{Z}$. Then clearly if $a \in \mathbb{Z}^*$ we have $a \sim a$ since $\frac{a^2+a}{a} = a + 1 \in \mathbb{Z}$. On the other hand, the relation is not symmetric, since $5 \sim 2$ as $\frac{5^2+5}{2} = 15 \in \mathbb{Z}$ but $2 \not\sim 5$, as $\frac{2^2+2}{5} = \frac{6}{5} \notin \mathbb{Z}$. It is not transitive either, since $\frac{5^2+5}{3} \in \mathbb{Z} \implies 5 \sim 3$ and $\frac{3^2+3}{12} \in \mathbb{Z} \implies 3 \sim 12$ but $\frac{5^2+5}{12} \notin \mathbb{Z}$ and so $5 \nsim 12$.

165 Definition Let $\sim$ be an equivalence relation on a set $\mathscr{S}$. Then the *equivalence class of a* is defined and denoted by

$$[a] = \{x \in \mathscr{S} : x \sim a\}.$$

166 Lemma Let $\sim$ be an equivalence relation on a set $\mathscr{S}$. Then two equivalence classes are either identical or disjoint.

Proof: *We prove that if $(a,b) \in \mathscr{S}^2$, and $[a] \cap [b] \neq \varnothing$ then $[a] = [b]$. Suppose that $x \in [a] \cap [b]$. Now $x \in [a] \implies x \sim a \implies a \sim x$, by symmetry. Similarly, $x \in [b] \implies x \sim b$. By transitivity*

$$(a \sim x) \textbf{ and } (x \sim b) \implies a \sim b.$$

Now, if $y \in [b]$ then $b \sim y$. Again by transitivity, $a \sim y$. This means that $y \in [a]$. We have shewn that $y \in [b] \implies y \in [a]$ and so $[b] \subseteq [a]$. In a similar fashion, we may prove that $[a] \subseteq [b]$. This establishes the result. ❑

As a way of motivating the following result, let us consider the following example. Suppose that a child is playing with 10 bricks, which come in 3 different colours and are numbered 1 through 10. Bricks 1 through 3 are red, bricks 4 through 7 are white and bricks 8 through 10 are blue.

Suppose we induce the relation $a \sim b$ whenever brick number a has the same colour as brick number b. The $\sim$ is clearly an equivalence relation and the bricks are partitioned according to colour. In this partition we have 3 classes (colours): bricks with numbers in $\{1,2,3\}$ belong to the "red" class; bricks with numbers in $\{4,5,6,7\}$ belong to the "white" class; and bricks with numbers in $\{8,9,10\}$ belong to the "blue" class.

Suppose that instead of grouping the bricks by colour we decided to group the bricks by the remainder given by the number of the brick upon division by 4, thus $a \approx b$ if a and b leave the same remainder upon division by 4. Clearly $\approx$ is also an equivalence relation. In this case bricks with numbers in $\{4,8\}$ belong to the "0" class; bricks with numbers in $\{1,5,9\}$ belong to the "1" class; bricks with numbers in $\{2,4,10\}$ belong to the "2" class; and bricks with numbers in $\{3,7\}$ belong to the "3" class.

Notice on the same set we constructed two different partitions, and that classes need not have the same number of elements.

167 Theorem Let $\mathscr{S} \neq \varnothing$ be a set. Any equivalence relation on $\mathscr{S}$ induces a partition of $\mathscr{S}$. Conversely, given a partition of $\mathscr{S}$ into disjoint, non-empty subsets, we can define an equivalence relation on $\mathscr{S}$ whose equivalence classes are precisely these subsets.

Proof: *By Lemma* **??**, *if* $\sim$ *is an equivalence relation on* $\mathscr{S}$ *then*

$$\mathscr{S} = \bigcup_{a \in S} [a],$$

and $[a] \cap [b] = \varnothing$ *if* $a \nsim b$. *This proves the first half of the theorem.*

Conversely, let

$$\mathscr{S} = \bigcup_{\alpha} S_\alpha, \;\; S_\alpha \cap S_\beta = \varnothing \;\text{ if } \alpha \neq \beta,$$

be a partition of $\mathscr{S}$. *We define the relation* $\approx$ *on* $\mathscr{S}$ *by letting* $a \approx b$ *if and only if they belong to the same* S_α. *Since the* S_α *are mutually disjoint, it is clear that* $\approx$ *is an equivalence relation on* $\mathscr{S}$ *and that for* $a \in S_\alpha$, *we have* $[a] = S_\alpha$. ❑

4.2 Functions

168 Definition By a *function* $f : \mathbf{Dom}(f) \to \mathbf{Target}(f)$ we mean the collection of the following ingredients:

❶ a *name* for the function. Usually we use the letter f.

❷ a set of inputs called the *domain* of the function. The domain of f is denoted by $\mathbf{Dom}(f)$.

❸ an *input parameter* , also called *independent variable* or *dummy variable*. We usually denote a typical input by the letter x.

❹ a set of possible outputs of the function, called the *target set* of the function. The target set of f is denoted by $\mathbf{Target}(f)$.

❺ an *assignment rule* or *formula*, assigning to **every input** a **unique** output. This assignment rule for f is usually denoted by $x \mapsto f(x)$. The output of x under f is also referred to as the *image of* x *under* f, and is denoted by $f(x)$.

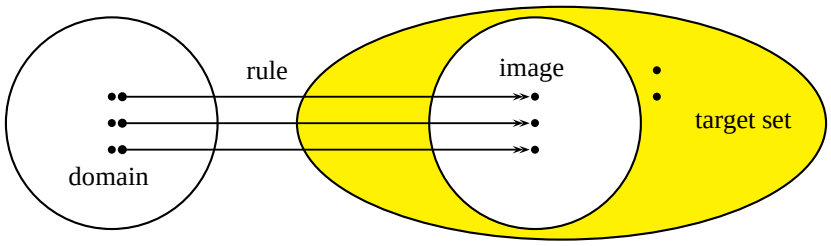

Figure 4.1: The main ingredients of a function.

The notation[1]

$$f: \begin{array}{ccc} \mathbf{Dom}(f) & \to & \mathbf{Target}(f) \\ x & \mapsto & f(x) \end{array}$$

read "the function f, with domain $\mathbf{Dom}(f)$, target set $\mathbf{Target}(f)$, and assignment rule f mapping x to $f(x)$" conveys all the above ingredients. See figure **??**.

169 Definition The *image* $\mathbf{Im}(f)$ of a function f is its set of actual outputs. In other words,

$$\mathbf{Im}(f) = \{f(a) : a \in \mathbf{Dom}(f)\}.$$

Observe that we always have $\mathbf{Im}(f) \subseteq \mathbf{Target}(f)$.

It must be emphasised that the uniqueness of the image of an element of the domain is crucial. For example, the diagram in figure **??** *does not* represent a function. The element 1 in the domain is assigned to more than one element of the target set. Also important in the definition of a function is the fact that *all the elements* of the domain must be operated on. For example, the diagram in **??** *does not* represent a function. The element 3 in the domain is not assigned to any element of the target set.

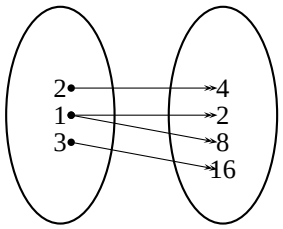

Figure 4.2: Not a function.

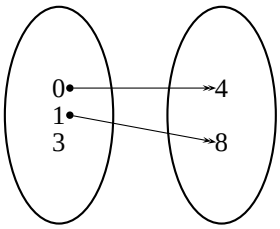

Figure 4.3: Not a function.

170 Example Consider the sets $A = \{1,2,3\}$, $B = \{1,4,9\}$, and the rule f given by $f(x) = x^2$, which means that f takes an input and squares it. Figures **??** through **??** give three ways of representing the function $f : A \to B$.

$$f: \begin{array}{ccc} \{1,2,3\} & \to & \{1,4,9\} \\ x & \mapsto & x^2 \end{array}$$

Figure 4.4: Example **??**.

$$f: \begin{pmatrix} 1 & 2 & 3 \\ 1 & 4 & 9 \end{pmatrix}$$

Figure 4.5: Example **??**.

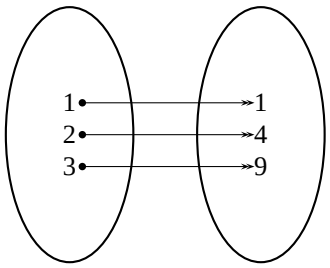

Figure 4.6: Example **??**.

171 Example Find all functions with domain $\{a,b\}$ and target set $\{c,d\}$.

Solution: There are $2^2 = 4$ such functions, namely:

❶ f_1 given by $f_1(a) = f_1(b) = c$. Observe that $\mathbf{Im}(f_1) = \{c\}$.

❷ f_2 given by $f_2(a) = f_2(b) = d$. Observe that $\mathbf{Im}(f_2) = \{d\}$.

❸ f_3 given by $f_3(a) = c$, $f_3(b) = d$. Observe that $\mathbf{Im}(f_3) = \{c,d\}$.

[1] Notice the difference in the arrows. The straight arrow $\longrightarrow$ is used to mean that a certain set is associated with another set, whereas the arrow $\mapsto$ (read "maps to") is used to denote that an input becomes a certain output.

❹ f_4 given by $f_4(a)=d, f_4(b)=c$. Observe that $\mathbf{Im}(f_4)=\{c,d\}$.

172 Definition A function is *injective* or *one-to-one* whenever two different values of its domain generate two different values in its image. A function is *surjective* or *onto* if every element of its target set is hit, that is, the target set is the same as the image of the function. A function is *bijective* if it is both injective and surjective.

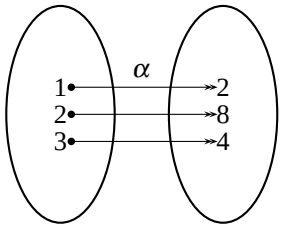

Figure 4.7: An injection.

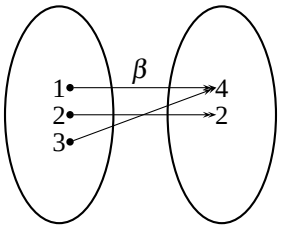

Figure 4.8: Not an injection

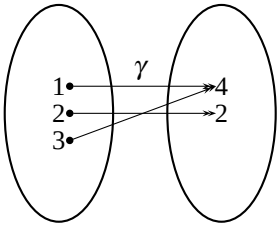

Figure 4.9: A surjection

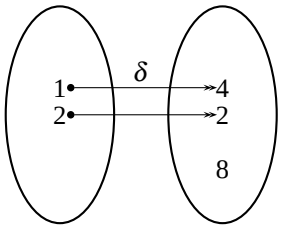

Figure 4.10: Not a surjection

173 Example The function α in the diagram **??** is an injective function. The function represented by the diagram **??**, however is not injective, since $\beta(3)=\beta(1)=4$, but $3\neq 1$. The function γ represented by diagram **??** is surjective. The function δ represented by diagram **??** is not surjective since 8 is part of the target set but not of the image of the function.

174 Theorem Let $f:A\to B$ be a function, and let A and B be finite. If f is injective, then $\mathrm{card}(A)\leq\mathrm{card}(B)$. If f is surjective then $\mathrm{card}(B)\leq\mathrm{card}(A)$. If f is bijective, then $\mathrm{card}(A)=\mathrm{card}(B)$.

Proof: *Put $n=\mathrm{card}(A)$, $A=\{x_1,x_2,\ldots,x_n\}$ and $m=\mathrm{card}(B)$, $B=\{y_1,y_2,\ldots,y_m\}$.*

If f were injective then $f(x_1),f(x_2),\ldots,f(x_n)$ are all distinct, and among the y_k. Hence $n\leq m$.

If f were surjective then each y_k is hit, and for each, there is an x_i with $f(x_i)=y_k$. Thus there are at least m different images, and so $n\geq m$. ❑

175 Definition A *permutation* is a function from a finite set to itself which reorders the elements of the set.

☞ *By necessity then, permutations are bijective.*

176 Example The following are permutations of $\{a,b,c\}$:

$$f_1:\begin{pmatrix}a&b&c\\a&b&c\end{pmatrix}\qquad f_2:\begin{pmatrix}a&b&c\\b&c&a\end{pmatrix}.$$

The following are *not* permutations of $\{a,b,c\}$:

$$f_3:\begin{pmatrix}a&b&c\\a&a&c\end{pmatrix}\qquad f_4:\begin{pmatrix}a&b&c\\b&b&a\end{pmatrix}.$$

177 Theorem Let A, B be finite sets with $\mathrm{card}(A)=n$ and $\mathrm{card}(B)=m$. Then

- the number of functions from A to B is m^n.
- if $n\leq m$, the number of injective functions from A to B is $m(m-1)(m-2)\cdots(m-n+1)$. If $n>m$ there are no injective functions from A to B.

Proof: *Each of the n elements of A must be assigned an element of B, and hence there are $\underbrace{m\cdot m\cdots m}_{n\text{ factors}}=m^n$ possibilities, and thus m^n functions.If a function from A to B is injective then we must have $n\leq m$ in view of Theorem **??**. If to different inputs*

we must assign different outputs then to the first element of A we may assign any of the m elements of B, to the second any of the $m-1$ remaining ones, to the third any of the $m-2$ remaining ones, etc., and so we have $m(m-1)\cdots(m-n+1)$ injective functions. ❑

178 Example Let $A=\{a,b,c\}$ and $B=\{1,2,3,4\}$. Then according to Theorem **??**, there are $4^3=64$ functions from A to B and of these, $4\cdot 3\cdot 2=24$ are injective. Similarly, there are $3^4=81$ functions from B to A, and none are injective.

179 Example Find the number of surjections from $A=\{a,b,c,d\}$ to $B=\{1,2,3\}$.

Solution: The trick here is that we know how to count the number of functions from one finite set to the other (Theorem **??**). What we do is over count the number of functions, and then sieve out those which are not surjective by means of Inclusion-Exclusion. By Theorem **??**, there are $3^4=81$ functions from A to B. There are $\binom{3}{1}2^4=48$ functions from A to B that miss one element from B. There are $\binom{3}{2}1^4=3$ functions from A to B that miss two elements from B. There are $\binom{3}{0}0^4=4$ functions from A to B that miss three elements from B. By Inclusion-Exclusion there are

$$81-48+3=36$$

surjective functions from A to B.

In analogy to example **??**, we may prove the following theorem, which complements Theorem **??** by finding the number of surjections from one set to another set.

180 Theorem Let A and B be two finite sets with $\text{card}(A)=n$ and $\text{card}(B)=m$. If $n<m$ then there are no surjections from A to B. If $n\geq m$ then the number of surjective functions from A to B is

$$m^n-\binom{m}{1}(m-1)^n+\binom{m}{2}(m-2)^n-\binom{m}{3}(m-3)^n+\cdots+(-1)^{m-1}\binom{m}{m-1}(1)^n.$$

Chapter 5

Number Theory

5.1 Division Algorithm

181 Definition If $a \neq 0, b$ are integers, we say that *a divides b* if there is an integer c such that $ac = b$. We write this as $a|b$.

If a does not divide b we write $a \not| b$.

182 Example Since $20 = 4 \cdot 5$ we have $4|20$. Also $-4|20$ since $20 = (-4)(-5)$.

183 Theorem Let a, b, c be integers.

1. If $a|b$ then $a|kb$ for any $k \in \mathbb{Z}$.
2. If $a|b$ and $b|a$, then $a = \pm b$.
3. If $a|b$ and $b|c$ then $a|c$.
4. If c divides a and b then c divides any linear combination of a and b. That is, if a, b, c, m, n are integers with $c|a, c|b$, then $c|(am+nb)$.
5. For any $k \in \mathbb{Z} \setminus \{0\}$, $a|b \iff ka|kb$.
6. If $a|b$ and $b \neq 0$ then $1 \leq |a| \leq |b|$.

Proof: *We prove the assertions in the given order.*

1. *There is $u \in \mathbb{Z}$ such that $au = b$. Then $a(uk) = bk$ and so $a|bk$.*
2. *Observe that by definition, neither $a \neq 0$ nor $b \neq 0$ if $a|b$ and $b|a$. There exist integers u, u' with $au = b$ and $bu' = a$. Hence $auu' = bu' = a$, and so $uu' = 1$. Since u, u' are integers, then $u = \pm 1, u' = \mp 1$. Hence $a = \pm b$.*
3. *There are integers u, v with $au = b, bv = c$. Hence $auv = c$, and so $a|c$.*
4. *There are integers s, t with $sc = a, tc = b$. Thus*

$$am + nb = c(sm + tn),$$

   giving $c|(am + bn)$.
5. *There exist an integer u with $au = b$. Then $(ak)u = kb$, and so $a|b \implies ka|kb$. Since $k \neq 0$ we may cancel out the k's and hence $(ak)u = kb \implies au = b \implies a|b$, proving the converse.*
6. *Since $b \neq 0$ there exists an integer $u \neq 0$ with $au = b$. So $|u| \geq 1$ and thus $|a| \cdot 1 \leq |a| \cdot |u| = |au| = |b|$. $|a| \geq 1$ trivially.*

❑

184 Theorem (Division Algorithm) Let $n > 0$ be an integer. Then for any integer a there exist unique integers q (called the *quotient*) and r (called the *remainder*) such that $a = qn + r$ and $0 \leq r < q$.

Proof: *In the proof of this theorem, we use the following property of the integers, called the* well-ordering principle*: any non-empty set of non-negative integers has a smallest element.*

Consider the set $S = \{a - bn : b \in \mathbb{Z} \text{ and } a \geq bn\}$. Then S is a collection of nonnegative integers and $S \neq \varnothing$ as $\pm a - 0 \cdot n \in S$ and this is non-negative for one choice of sign. By the Well-Ordering Principle, S has a least element, say r. Now, there must be some $q \in \mathbb{Z}$ such that $r = a - qn$ since $r \in S$. By construction, $r \geq 0$. Let us prove that $r < n$. For assume that $r \geq n$. Then $r > r - n = a - qn - n = a - (q+1)n \geq 0$, since $r - n \geq 0$. But then $a - (q+1)n \in S$ and $a - (q+1)n < r$ which contradicts the fact that r is the smallest member of S. Thus we must have $0 \leq r < n$. To prove that r and q are unique, assume that $q_1 n + r_1 = a = q_2 n + r_2$, $0 \leq r_1 < n$, $0 \leq r_2 < n$. Then $r_2 - r_1 = n(q_1 - q_2)$, that is, n divides $(r_2 - r_1)$. But $|r_2 - r_1| < n$, whence $r_2 = r_1$. From this it also follows that $q_1 = q_2$. This completes the proof. ❑

185 Example If $n = 5$ the Division Algorithm says that we can arrange all the integers in five columns as follows:

$$\begin{array}{rrrrr} \vdots & \vdots & \vdots & \vdots & \vdots \\ -10 & -9 & -8 & -7 & -6 \\ -5 & -4 & -3 & -2 & -1 \\ 0 & 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 & 9 \\ \vdots & \vdots & \vdots & \vdots & \vdots \end{array}$$

The arrangement above shews that any integer comes in one of 5 flavours: those leaving remainder 0 upon division by 5, those leaving remainder 1 upon division by 5, etc. We let

$$5\mathbb{Z} = \{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\} = \overline{0},$$

$$5\mathbb{Z}+1 = \{\ldots, -14, -9, -4, 1, 6, 11, 16, \ldots\} = \overline{1},$$
$$5\mathbb{Z}+2 = \{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots\} = \overline{2},$$
$$5\mathbb{Z}+3 = \{\ldots, -12, -7, -2, 3, 8, 13, 18, \ldots\} = \overline{3},$$
$$5\mathbb{Z}+4 = \{\ldots, -11, -6, -1, 4, 9, 14, 19, \ldots\} = \overline{4},$$

and

$$\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}.$$

186 Example Shew that $n^2 + 23$ is divisible by 24 for infinitely many values of n.

Solution: Observe that $n^2 + 23 = n^2 - 1 + 24 = (n-1)(n+1) + 24$. Therefore the families of integers $n = 24m \pm 1, m = 0, \pm 1, \pm 2, \pm 3, \ldots$ produce infinitely many values such that $n^2 + 23$ is divisible by 24.

187 Example Shew that the square of any prime greater than 3 leaves remainder 1 upon division by 12.

Solution: If $p > 3$ is prime, then p is of one of the forms $6k \pm 1$.

Now,

$$(6k \pm 1)^2 = 12(3k^2 \pm k) + 1,$$

proving the assertion.

188 Example Prove that if p is a prime, then one of $8p - 1$ and $8p + 1$ is a prime and the other is composite.

Solution: If $p = 3$, $8p - 1 = 23$ and $8p + 1 = 25$, then the assertion is true for $p = 3$. If $p > 3$, then either $p = 3k + 1$ or $p = 3k + 2$. If $p = 3k + 1$, $8p - 1 = 24k - 7$ and $8p + 1 = 24k - 6$, which is divisible by 6 and hence not prime. If $p = 3k + 2$, $8p - 1 = 24k - 15$ is not a prime, .

189 Example (AHSME 1976) Let r be the common remainder when $1059, 1417$ and 2312 are divided by $d > 1$. Find $d - r$.

Solution: By the division algorithm there are integers q_1, q_2, q_3 with $1059 = dq_1 + r, 1417 = dq_2 + r$ and $2312 = dq_3 + r$. Subtracting we get $1253 = d(q_3 - q_1), 895 = d(q_3 - q_2)$ and $358 = d(q_2 - q_1)$. Notice that d is a common divisor of $1253, 895$, and 358. As $1253 = 7 \cdot 179$, $895 = 5 \cdot 179$, and $358 = 2 \cdot 179$, we see that 179 is the common divisor greater than 1 of all three quantities, and so $d = 179$. Since $1059 = 179q_1 + r$, and $1059 = 5 \cdot 179 + 164$, we deduce that $r = 164$. Finally, $d - r = 15$.

190 Example Shew that if $3n + 1$ is a square, then $n + 1$ is the sum of three squares.

Solution: Clearly $3n+1$ is not a multiple of 3, and so $3n+1=(3k\pm1)^2$. Therefore

$$n+1=\frac{(3k\pm1)^2-1}{3}+1=3k^2\pm2k+1=k^2+k^2+(k\pm1)^2,$$

as we wanted to shew.

5.2 Greatest Common Divisor

191 Definition Let a, b be integers with one of them different from 0. The greatest common divisor d of a,b, denoted by $d=\gcd(a,b)$ is the largest positive integer that divides both a and b.

192 Theorem (Bachet-Bezout Theorem) The greatest common divisor of any two integers a,b can be written as a linear combination of a and b, i.e., there are integers x,y with

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

Proof: *Let $A=\{ax+by|ax+by>0,x,y\in\mathbb{Z}\}$. Clearly one of $\pm a,\pm b$ is in A, as both a,b are not zero. By the Well Ordering Principle, A has a smallest element, say d. Therefore, there are x_0,y_0 such that $d=ax_0+by_0$. We prove that $d=\gcd(a,b)$. To do this we prove that d divides a and b and that if t divides a and b, then t must also divide then d.*

We first prove that d divides a. By the Division Algorithm, we can find integers $q,r,0\le r<d$ such that $a=dq+r$. Then

$$r=a-dq=a(1-qx_0)-by_0.$$

If $r>0$, then $r\in A$ is smaller than the smaller element of A, namely d, a contradiction. Thus $r=0$. This entails $dq=a$, i.e. d divides a. We can similarly prove that d divides b.

Assume that t divides a and b. Then $a=tm,b=tn$ for integers m,n. Hence $d=ax_0+bx_0=t(mx_0+ny_0)$, that is, t divides d. The theorem is thus proved. ❑

Let a,b be positive integers. After using the Division Algorithm repeatedly, we find the sequence of equalities

$$\begin{array}{lcll} a & = & bq_1+r_2, & 0<r_2<b,\\ b & = & r_2q_2+r_3 & 0<r_3<r_2,\\ r_2 & = & r_3q_3+r_4 & 0<r_4<r_3,\\ \vdots & \vdots & \vdots & \vdots\\ r_{n-2} & = & r_{n-1}q_{n-1}+r_n & 0<r_n<r_{n-1},\\ r_{n-1} & = & r_nq_n. & \end{array} \tag{5.1}$$

The sequence of remainders will eventually reach a r_{n+1} which will be zero, since $b,r_2,r_3,\ldots$ is a monotonically decreasing sequence of integers, and cannot contain more than b positive terms.

The Euclidean Algorithm rests on the fact, to be proved below, that $\gcd(a,b)=\gcd(b,r_2)=\gcd(r_2,r_3)=\cdots=\gcd(r_{n-1},r_n)=r_n$.

193 Theorem If r_n is the last non-zero remainder found in the process of the Euclidean Algorithm, then

$$r_n=\gcd(a,b).$$

Proof: *From equations* **??**

$$\begin{array}{lcl} r_2 & = & a-bq_1\\ r_3 & = & b-r_2q_2\\ r_4 & = & r_2-r_3q_3\\ \vdots & \vdots & \vdots\\ r_n & = & r_{n-2}-r_{n-1}q_{n-1} \end{array}$$

Let $r=\gcd(a,b)$. From the first equation, $r|r_2$. From the second equation, $r|r_3$. Upon iterating the process, we see that $r|r_n$. But starting at the last equation **??** *and working up, we see that $r_n|r_{n-1},r_n|r_{n-2},\ldots r_n|r_2,r_n|b,r_n|a$. Thus r_n is a common divisor of a and b and so $r_n|\gcd(a,b)$. This gives the desired result.* ❑

194 Example Write pseudocode describing the Euclidean Algorithm.

Solution: Here is one iterative way of doing this.

Algorithm 5.2.1: EUCLIDEANALGORITHM(x,y)

if $x<0$
  then $x\leftarrow -x$
if $y<0$
  then $y\leftarrow -y$
while $y>0$
  do $\begin{cases} r\leftarrow x \mod y \\ x\leftarrow y \\ y\leftarrow r \end{cases}$

195 Example Find $\gcd(23,29)$ by means of the Euclidean Algorithm.

Solution: We have

$$29=1\cdot 23+6,$$
$$23=3\cdot 6+5,$$
$$6=1\cdot 5+1,$$
$$5=5\cdot 1.$$

The last non-zero remainder is 1, thus $\gcd(23,29)=1$.

An equation which requires integer solutions is called a *diophantine equation*. By the Bachet-Bezout Theorem **??**, we see that the linear diophantine equation

$$ax+by=c$$

has a solution in integers if and only if $\gcd(a,b)|c$. The Euclidean Algorithm is an efficient means to find a solution to this equation.

196 Example Find integers x,y that satisfy the linear diophantine equation

$$23x+29y=1.$$

Solution: We work upwards, starting from the penultimate equality in the preceding problem:

$$1=6-1\cdot 5,$$
$$5=23-3\cdot 6,$$
$$6=29\cdot 1-23.$$

Hence,

$$\begin{aligned} 1 &= 6-1\cdot 5 \\ &= 6-1\cdot(23-3\cdot 6) \\ &= 4\cdot 6-1\cdot 23 \\ &= 4(29\cdot 1-23)-1\cdot 23 \\ &= 4\cdot 29-5\cdot 23. \end{aligned}$$

This solves the equation, with $x=-5, y=4$.

197 Example Find integer solutions to

$$23x+29y=7.$$

Solution: From the preceding example, $23(-5)+29(4)=1$. Multiplying both sides of this equality by 7,

$$23(-35)+29(28)=7,$$

which solves the problem.

198 Example Find infinitely many integer solutions to

$$23x+29y=1.$$

Solution: By example **??**, the pair $x_0 = -5, y_0 = 4$ is a solution. We can find a family of solutions by letting

$$x = -5 + 29t,\ y = 4 - 23t,\ \ t \in \mathbb{Z}.$$

199 Example Can you find integers x, y such that $3456x + 246y = 73$?

Solution: No. $(3456, 246) = 2$ and $2 \not| 73$.

5.3 Non-decimal Scales

The fact that most people have ten fingers has fixed our scale of notation to the decimal. Given any positive integer $r > 1$, we can, however, express any number x in base r.

If n is a positive integer, and $r > 1$ is an integer, then n has the base-r representation

$$n = a_0 + a_1 r + a_2 r^2 + \cdots + a_k r^k,\ 0 \leq a_t \leq r-1,\ a_k \neq 0,\ r^k \leq n < r^{k+1}.$$

We use the convention that we shall refer to a decimal number without referring to its base, and to a base-r number by using the subindex r.

200 Example Express the decimal number 5213 in base-seven.

Solution: Observe that $5213 < 7^5$. We thus want to find $0 \leq a_0, \ldots, a_4 \leq 6, a_4 \neq 0$ such that

$$5213 = a_4 7^4 + a_3 7^3 + a_2 7^2 + a_1 7 + a_0.$$

Dividing by 7^4, we obtain $2+$ proper fraction $= a_4 +$ proper fraction. This means that $a_4 = 2$. Thus $5213 = 2 \cdot 7^4 + a_3 7^3 + a_2 7^2 + a_1 7 + a_0$ or $411 = 5213 = a_3 7^3 + a_2 7^2 + a_1 7 + a_0$. Dividing by 7^3 this last equality we obtain $1+$ proper fraction $= a_3 +$ proper fraction, and so $a_3 = 1$. Continuing in this way we deduce that $5213 = 21125_7$.

The method of successive divisions used in the preceding problem can be conveniently displayed as

7	5212	5
7	744	2
7	106	1
7	15	1
7	2	2

The central column contains the successive quotients and the rightmost column contains the corresponding remainders. Reading from the last remainder up, we recover $5213 = 21125_7$.

201 Example Write 562_7 in base-five.

Solution: $562_7 = 5 \cdot 7^2 + 6 \cdot 7 + 2 =$ in decimal scale, so the problem reduces to convert 289 to base-five. Doing successive divisions,

5	289	4
5	57	2
5	11	1
5	2	2

Thus $562_7 = 289 = 2124_5$.

202 Example Express the fraction $\frac{13}{16}$ in base-six.

Solution: Write

$$\frac{13}{16} = \frac{a_1}{6} + \frac{a_2}{6^2} + \frac{a_3}{6^3} + \frac{a_4}{6^4} + \cdots$$

Multiplying by 6, we obtain $4+$ proper fraction $= a_1 +$ proper fraction, so $a_1 = 4$. Hence

$$\frac{13}{16} - \frac{4}{6} = \frac{7}{48} = \frac{a_2}{6^2} + \frac{a_3}{6^3} + \frac{a_4}{6^4} + \cdots$$

Multiply by 6^2 we obtain $5+$ proper fraction $= a_2+$ proper fraction, and so $a_2 = 5$. Continuing in this fashion

$$\frac{13}{16} = \frac{4}{6} + \frac{5}{6^2} + \frac{1}{6^3} + \frac{3}{6^4} = 0.4513_6.$$

We may simplify this procedure of successive multiplications by recurring to the following display:

6	$\frac{13}{16}$	4
6	$\frac{7}{8}$	5
6	$\frac{1}{4}$	1
6	$\frac{1}{2}$	3

The third column contains the integral part of the products of the first column and the second column. Each term of the second column from the second on is the fractional part of the product obtained in the preceding row. Thus $6 \cdot \frac{13}{16} - 4 = \frac{7}{8}$, $6 \cdot \frac{7}{8} - 5 = \frac{1}{4}$, etc..

203 Example Prove that 4.41_r is a perfect square in any scale of notation.

Solution:

$$4.41_r = 4 + \frac{4}{r} + \frac{4}{r^2} = \left(2 + \frac{1}{r}\right)^2$$

204 Example (AIME 1986) The increasing sequence

$$1, 3, 4, 9, 10, 12, 13, \ldots$$

consists of all those positive integers which are powers of 3 or sums of distinct powers or 3. Find the hundredth term of the sequence.

Solution: If the terms of the sequence are written in base-three, they comprise the positive integers which do not contain the digit 2. Thus the terms of the sequence in ascending order are

$$1_3, 10_3, 11_3, 100_3, 101_3, 110_3, 111_3, \ldots$$

In the *binary* scale these numbers are, of course, the ascending natural numbers $1, 2, 3, 4, \ldots$. Therefore to obtain the 100th term of the sequence we write 100 in binary and then translate this into ternary: $100 = 1100100_2$ and $1100100_3 = 3^6 + 3^5 + 3^2 = 981$.

5.4 Congruences

205 Definition Let $n > 0$ be an integer. We say that "a is congruent to b modulo n" written $a \equiv b \mod n$ if a and b leave the same remainder upon division by n.

206 Example

$$-8 \equiv 6 \mod 7,$$
$$-8 \equiv 13 \mod 7.$$

By the division algorithm any integer a can be written as $a = qn + r$ with $0 \leq r < n$. By letting q vary over the integers we obtain the arithmetic progression

$$\ldots, r - 3n, r - 2n, r - n, r, r + n, r + 2n, r + 3n, \ldots,$$

and so all the numbers in this sequence are congruent to a modulo n.

207 Theorem Let $n > 0$ be an integer. Then $a \equiv b \mod n \iff n|(a - b)$.

Proof: *Assume $a \neq b$, otherwise the result is clear. By the Euclidean Algorithm there are integers $q_1 \neq q_2$ such that $a = q_1 n + r$ and $b = q_2 n + r$, as a and b leave the same remainder when divided by n. Thus $a - b = q_1 n - q_2 n = (q_1 - q_2)n$. This implies that $n|(a - b)$.*

Conversely if $n|(a-b)$ then there is an integer t such that $nt = a-b$. Assume that $a = m_1 n + r_1$ and $b = m_2 n + r_2$ with $0 \le r_1, r_2 < n$. Then

$$nt = a-b = (m_1-m_2)n + r_1 - r_2 \implies n(t-m_1+m_2) = r_1 - r_2 \implies n|(r_1-r_2).$$

Since $|r_1 - r_2| < n$ we must have $r_1 - r_2 = 0$ and so a and b leave the same remainder upon division by n. ❑

We now provesome simple properties of congruences.

208 Theorem Let $a, b, c, d, m \in \mathbb{Z}, k \in$ with $a \equiv b \mod m$ and $c \equiv d \mod m$. Then

1. $a + c \equiv b + d \mod m$
2. $a - c \equiv b - d \mod m$
3. $ac \equiv bd \mod m$
4. $a^k \equiv b^k \mod m$
5. If f is a polynomial with integral coefficients then $f(a) \equiv f(b) \mod m$.

Proof: *As $a \equiv b \mod m$ and $c \equiv d \mod m$, we can find $k_1, k_2 \in \mathbb{Z}$ with $a = b + k_1 m$ and $c = d + k_2 m$. Thus $a \pm c = b \pm d + m(k_1 \pm k_2)$ and $ac = bd + m(k_2 b + k_1 d)$. These equalities give (1), (2) and (3). Property (4) follows by successive application of (3), and (5) follows from (4).* ❑

Congruences mod 9 can sometimes be used to check multiplications. For example $875961 \cdot 2753 \neq 2410520633$. For if this were true then

$$(8+7+5+9+6+1)(2+7+5+3) \equiv 2+4+1+0+5+2+0+6+3+3 \mod 9.$$

But this says that $0 \cdot 8 \equiv 8 \mod 9$, which is patently false.

209 Example Find the remainder when 6^{1987} is divided by 37.

Solution: $6^2 \equiv -1 \mod 37$. Thus $6^{1987} \equiv 6 \cdot 6^{1986} \equiv 6(6^2)^{993} \equiv 6(-1)^{993} \equiv -6 \equiv 31 \mod 37$.

210 Example Prove that 7 divides $3^{2n+1} + 2^{n+2}$ for all natural numbers n.

Solution: Observe that $3^{2n+1} \equiv 3 \cdot 9^n \equiv 3 \cdot 2^n \mod 7$ and $2^{n+2} \equiv 4 \cdot 2^n \mod 7$. Hence

$$3^{2n+1} + 2^{n+2} \equiv 7 \cdot 2^n \equiv 0 \mod 7,$$

for all natural numbers n.

211 Example Prove that $7|(2222^{5555} + 5555^{2222})$.

Solution: $2222 \equiv 3 \mod 7$, $5555 \equiv 4 \mod 7$ and $3^5 \equiv 5 \mod 7$. Now

$$2222^{5555} + 5555^{2222} \equiv 3^{5555} + 4^{2222} \equiv (3^5)^{1111} + (4^2)^{1111} \equiv 5^{1111} - 5^{1111} \equiv 0 \mod 7.$$

212 Example Find the units digit of 7^{7^7}.

Solution: We must find $7^{7^7} \mod 10$. Now, $7^2 \equiv -1 \mod 10$, and so $7^3 \equiv 7^2 \cdot 7 \equiv -7 \equiv 3 \mod 10$ and $7^4 \equiv (7^2)^2 \equiv 1 \mod 10$. Also, $7^2 \equiv 1 \mod 4$ and so $7^7 \equiv (7^2)^3 \cdot 7 \equiv 3 \mod 4$, which means that there is an integer t such that $7^7 = 3 + 4t$. Upon assembling all this,

$$7^{7^7} \equiv 7^{4t+3} \equiv (7^4)^t \cdot 7^3 \equiv 1^t \cdot 3 \equiv 3 \mod 10.$$

Thus the last digit is 3.

213 Example Prove that every year, including any leap year, has at least one Friday 13th.

Solution: It is enough to prove that each year has a Sunday the 1st. Now, the first day of a month in each year falls in one of the following days:

Month	Day of the year	mod 7
January	1	1
February	32	4
March	60 or 61	4 or 5
April	91 or 92	0 or 1
May	121 or122	2 or 3
June	152 or 153	5 or 6
July	182 or183	0 or 1
August	213 or 214	3 or 4
September	244 or 245	6 or 0
October	274 or 275	1 or 2
November	305 or 306	4 or 5
December	335 or 336	6 or 0

(The above table means that, depending on whether the year is a leap year or not, that March 1st is the 50th or 51st day of the year, etc.) Now, each remainder class modulo 7 is represented in the third column, thus each year, whether leap or not, has at least one Sunday the 1st.

214 Example Find infinitely many integers n such that 2^n+27 is divisible by 7.

Solution: Observe that $2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 1, 2^4 \equiv 2, 2^5 \equiv 4, 2^6 \equiv 1 \mod 7$ and so $2^{3k} \equiv 1 \mod 3$ for all positive integers k. Hence $2^{3k}+27 \equiv 1+27 \equiv 0 \mod 7$ for all positive integers k. This produces the infinitely many values sought.

215 Example Prove that $2^k-5, k=0,1,2,\ldots$ never leaves remainder 1 when divided by 7.

Solution: $2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 1 \mod 7$, and this cycle of three repeats. Thus 2^k-5 can leave only remainders 3, 4, or 6 upon division by 7.

5.5 Divisibility Criteria

216 Theorem An integer n is divisible by 5 if and only if its last digit is a 0 or a 5.

Proof: *We derive the result for $n>0$, for if $n<0$ we simply apply the result to $-n>0$. Since $10^k \equiv 0 \mod 5$ for integral $k \geq 1$, we have*

$$n = a_s 10^s + a_{s-1}10^{s-1} + \cdots + a_1 10 + a_0 \equiv a_0 \mod 5,$$

Thus divisibility of n by 5 depends on whether a_0 is divisible by 5, which happens only when $a_0=0$ or $a_0=5$. ❑

217 Theorem Let k be a positive integer. An integer n is divisible by 2^k if and only if the number formed by the last k digits of n is divisible by 2^k.

Proof: *If $n=0$ there is nothing to prove. If we prove the result for $n>0$ then we can deduce the result for $n<0$ by applying it to $-n=(-1)n>0$. So assume that $n \in \mathbb{Z}$, $n>0$ and let its decimal expansion be*

$$n = a_s 10^s + a_{s-1}10^{s-1} + \cdots + a_1 10 + a_0,$$

where $0 \le a_i \le 9,\ a_s \neq 0$. *Now, each of* $10^t = 2^t 5^t \equiv 0 \mod 2^t$ *for* $t \ge k$. *Hence*

$$\begin{aligned} n &= a_s 10^s + a_{s-1}10^{s-1} + \cdots + a_1 10 + a_0 \\ &\equiv a_{k-1}10^{k-1} + a_{k-2}10^{k-2} + \cdots + a_1 10 + a_0 \mod 2^k, \end{aligned}$$

so n is divisible by 2^k *if and only if the number formed by the last k digits of n is divisible by* 2^k. ❑

218 Example The number 987654888 is divisible by $2^3 = 8$ because the number formed by its last three digits, 888 is divisible by 8.

219 Example The number 191919191919193216 is divisible by $2^4 = 16$ because the number formed by its last four digits, 3216 is divisible by 16.

220 Example By what digits may one replace A so that the integer 231A2 be divisible by 4?

Solution: The number 231A2 is divisible by 4 if and only if $A2$ is divisible by 4. This happens when $A = 1$ ($A2 = 12$), $A = 3$ ($A2 = 32$), $A = 5$ ($A2 = 52$), $A = 7$ ($A2 = 72$), and $A = 9$ ($A2 = 92$). Thus the five numbers

$$23112, 23132, 2315223172, 23192,$$

are all divisible by 4.

221 Example Determine digits a, b so that 235ab be divisible by 40.

Solution: 235ab will be divisible by 40 if and only if it is divisible by 8 and by 5. If 235ab is divisible by 8 then, *a fortiori*, it is even and since we also require it to be divisible by 5 we must have $b = 0$. Thus we need a digit a so that 5a0 be divisible by 8. Since $0 \le a \le 9$, a quick trial an error gives that the desired integers are

$$23500, 23520, 23540, 23560, 23580.$$

222 Theorem (Casting-out 9's) An integer n is divisible by 9 if and only if the sum of its digits is divisible by 9.

Proof: *If* $n = 0$ *there is nothing to prove. If we prove the result for* $n > 0$ *then we can deduce the result for* $n < 0$ *by applying it to* $-n = (-1)n > 0$. *So assume that* $n \in \mathbb{Z}$, $n > 0$ *and let its decimal expansion be*

$$n = a_s 10^s + a_{s-1}10^{s-1} + \cdots + a_1 10 + a_0,$$

where $0 \le a_i \le 9,\ a_s \neq 0$. *Observe that* $10 \equiv 1 \mod 9$ *and so* $10^t \equiv 1^t \equiv 1 \mod 9$. *Now*

$$\begin{aligned} n &= a_s 10^s + a_{s-1}10^{s-1} + \cdots + a_1 10 + a_0 \\ &\equiv a_s + \cdots + a_1 + a_0 \mod 9, \end{aligned}$$

from where the result follows. ❑

☞ *Since* $10 \equiv 1 \mod 3$ *we can also deduce that integer n is divisible by* 3 *if and only if the sum of it digits is divisible by* 3.

223 Example What values should the digit d take so that the number 32d5 be divisible by 9?

Solution: The number 32d5 is divisible by 9 if and only $3 + 2 + d + 5 = d + 10$ is divisible by 9. Now,

$$0 \le d \le 9 \implies 10 \le d + 10 \le 19.$$

The only number in the range 10 to 19 divisible by 9 is 18, thus $d = 8$. One can easily verify that 3285 is divisible by 9.

224 Example Is there a digit d so that 125d be divisible by 45?

Solution: If $125d$ were divisible by 45, it must be divisible by 9 and by 5. If it were divisible by 5, then $d = 0$ or $d = 5$. If $d = 0$, the digital sum is $1+2+5+0 = 8$, which is not divisible by 9. Similarly, if $d = 5$, the digital sum is $1+2+5+5 = 13$, which is neither divisible by 9. So $125d$ is never divisible by 45.

225 Definition If the positive integer n has decimal expansion

$$n = a_s 10^s + a_{s-1}10^{s-1} + \cdots + a_1 10 + a_0,$$

the *alternating digital sum* of n is

$$a_s - a_{s-1} + a_{s-2} - a_{s-3} + \cdots + (-1)^{s-1} a_0$$

226 Example The alternating digital sum of 135456 is

$$1-3+5-4+5-6 = -2.$$

227 Theorem An integer n is divisible by 11 if and only if its alternating digital sum is divisible by 11.

Proof: *We may assume that $n > 0$. Let*

$$n = a_s 10^s + a_{s-1}10^{s-1} + \cdots + a_1 10 + a_0,$$

where $0 \leq a_i \leq 9$, $a_s \neq 0$. Observe that $10 \equiv -1 \mod 11$ and so $10^t \equiv (-1) \mod 11$. Hence

$$\begin{aligned} n &= a_s 10^s + a_{s-1}10^{s-1} + \cdots + a_1 10 + a_0 \\ &\equiv a_s(-1)^s + a_{s-1}(-1)^{s-1} + a_{s-2}(-1)^{s-2} + \cdots + -a_1 + a_0 \mod 11 \end{aligned}$$

and the result follows from this. ❑

228 Example 912282219 has alternating digital sum $9-1+2-2+8-2+2-1+9 = 24$ and so 912282219 is not divisible by 11, whereas 8924310064539 has alternating digital sum $8-9+2-4+3-1+0-0+6-4+4-3+9 = 11$, and so 8924310064539 is divisible by 11.

Homework

229 Problem Prove that there are infinitely many integers n such that $4n^2+1$ is simultaneously divisible by 13 and 5.

230 Problem Find the least positive integer solution of the equation $436x - 393y = 5$.

231 Problem Two rods of equal length are divided into 250 and 243 equal parts, respectively. If their ends be coincident, find the divisions which are the nearest together.

232 Problem Prove that any integer $n > 11$ is the sum of two positive composite numbers.

233 Problem Let $n > 1$ be an integer.

1. Prove, using induction or otherwise, that if $a \neq 1$ then
$$1 + a + a^2 + \cdots a^{n-1} = \frac{1-a^n}{1-a}.$$
2. By making the substitution $a = \frac{x}{y}$ prove that
$$x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1}).$$
3. Deduce that if $x \neq y$ are integers then $(x-y)|x^n - y^n$.
4. Shew that
$$2903^n - 803^n - 464^n + 261^n$$
is divisible by 1897 for all natural numbers n.

5. Prove that if 2^n-1 is prime, then n must be prime.
6. Deduce that if $x \neq y$ are integers, and n is odd, then $(x+y)|x^n+y^n$.
7. Prove that if 2^n+1 is prime, then $n=2^k$ for some integer k.

234 Problem Use the preceding problem to find the prime factor $p > 250000$ of the integer

$$1002004008016032.$$

235 Problem Write an algorithm that finds integer solutions x,y to the equation

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

Assume that at least one of a or b is different from 0.

236 Problem Let A be a positive integer, and A' be a number written with the aid of the same digits with are arranged in some other order. Prove that if $A+A' = 10^{10}$, then A is divisible by 10.

237 Problem A grocer sells a 1-gallon container of milk for 79 cents (comment: those were the days!) and a half gallon container of milk for 41 cents. At the end of the day he sold $63.58 worth of milk. How many 1 gallon and half gallon containers did he sell?

238 Problem Using congruences, find the last two digits of 3^{100}. Hint: $3^{40} \equiv 1 \mod 100$.

Answers

229 We have $4n^2+1 = 4n^2-64+65 = 4(n-4)(n+4)+65$ so it is enough to take $n = 65k \pm 4$.

230 Using the Euclidean Algorithm,

$$\begin{aligned} 436 &= 1\cdot 393+43 \\ 393 &= 9\cdot 43+6 \\ 43 &= 7\cdot 6+1 \end{aligned}$$

Hence

$$\begin{aligned} 1 &= 43-7\cdot 6 \\ &= 43-7\cdot(393-9\cdot 43) \\ &= -7\cdot 393+64\cdot 43 \\ &= -7\cdot 393+64\cdot(436-393) \\ &= -71\cdot 393+64\cdot 436, \end{aligned}$$

and so $5 = 320\cdot 436-355\cdot 393$. An infinite set of solutions can be achieved by putting $x = 320+393t$, $y = 355+436t$.

231 Observe that $\gcd(243,250) = 1$, and so the divisions will be nearest together when they differ by the least amount, that is, we seek solutions of $243x-250y = \pm 1$. By using the Euclidean Algorithm we find $243\cdot 107-250\cdot 104 = 1$ and also $243\cdot(250-107)-250\cdot(243-104) = -1$ and so the values of x are 107 and 143 and those of y are 104 and 139.

232 If $n > 11$ is even then $n-6$ is even and at least $12-4 = 8$ and thus it is composite. Hence $n = (n-6)+6$ is the sum of two even composite numbers. If $n > 11$ is odd then $n-9$ is even at least $13-9 = 4$, and hence composite. Therefore $n = (n-9)+9$ of an even and an odd composite number.

233 1. Put $S = 1+a+a^2+\cdots+a^{n-1}$. Then $aS = a+a^2+\cdots+a^{n-1}+a^n$. Thus $S-aS = (1+a+a^2+\cdots+a^{n-1})-(a+a^2+\cdots+a^{n-1}+a^n) = 1-a^n$, and from $(1-a)S = S-aS = 1-a^n$ we obtain the result.

2. From

$$1+\frac{x}{y}+\left(\frac{x}{y}\right)^2+\cdots+\left(\frac{x}{y}\right)^{n-1}=\frac{1-\left(\frac{x}{y}\right)^n}{1-\frac{x}{y}}$$

we obtain

$$\left(1-\frac{x}{y}\right)\left(1+\frac{x}{y}+\left(\frac{x}{y}\right)^2+\cdots+\left(\frac{x}{y}\right)^{n-1}\right)=1-\left(\frac{x}{y}\right)^n,$$

and multiplying by y^n both sides gives the result.

3. This is immediate from the above result.

4. By the preceding part, 2903^n-803^n is divisible by $2903-803=2100=7\cdot 300=$, and 261^n-464^n is divisible by $261-464=-203=7\cdot(-29)$. Thus the expression $2903^n-803^n-464^n+261^n$ is divisible by 7. Also, 2903^n-464^n is divisible by $2903-464=9\cdot 271$ and 261^n-803^n is divisible by $-542=(-2)271$. Thus the expression is also divisible by 271. Since 7 and 271 have no prime factors in common, we can conclude that the expression is divisible by $7\cdot 271=1897$.

5. We have

$$2^n-1=2^{ab}-1=(2^a-1)((2^a)^{b-1}+(2^a)^{b-2}+\cdots+(2^a)^1+1).$$

Since $a>1, 2^a-1>1$. Since $b>1$,

$$(2^a)^{b-1}+(2^a)^{b-2}+\cdots(2^a)^1+1)\geq 2^a+1>1.$$

We have decomposed a prime number (the left hand side) into the product of two factors, each greater than 1, a contradiction. Thus n must be a prime. Primes of this form are called *Mersenne primes.*

6. For every n we have that $x-y$ divides x^n-y^n. By changing y into $-y$ we deduce that $x-(-y)$ divides $x^n-(-y)^n$, that is $x+y$ divides $x^n-(-y)^n$. If n is odd then $-(-y)^n=y^n$, which gives the result.

7. We have

$$2^n+1=2^{2^k m}+1=(2^{2^k}+1)((2^{2^k})^{m-1}-(2^{2^k})^{m-2}+\cdots-(2^{2^k})^1+1).$$

Clearly, $2^{2^k}+1>1$. Also if $m\geq 3$

$$(2^{2^k})^{m-1}-(2^{2^k})^{m-2}+\cdots-(2^{2^k})^1+1\geq(2^{2^k})^2-(2^{2^k})^1+1>1,$$

and so, we have produced two factors each greater than 1 for the prime 2^n+1, which is nonsense. Primes of this form are called *Fermat primes.*

234 If $a=10^3, b=2$ then

$$1002004008016032=a^5+a^4b+a^3b^2+a^2b^3+ab^4+b^5=\frac{a^6-b^6}{a-b}.$$

This last expression factorises as

$$\begin{aligned}\frac{a^6-b^6}{a-b} &= (a+b)(a^2+ab+b^2)(a^2-ab+b^2)\\ &= 1002\cdot 1002004\cdot 998004\\ &= 4\cdot 4\cdot 1002\cdot 250501\cdot k,\end{aligned}$$

where $k<250000$. Therefore $p=250501$.

235 Here a possible approach. I have put semicolons instead of writing the algorithm strictly vertically in order to save space.

Algorithm 5.5.1: LINEARDIOPHANTINE(a,b)

$m \leftarrow a;\ \ n \leftarrow b;\ \ p \leftarrow 1;\ \ q \leftarrow 0;\ \ r \leftarrow 0;\ \ s \leftarrow 1;$

while $\neg((m=0)\vee(n=0))$

$$\begin{cases} \textbf{if } m \geq n \\ \quad \textbf{then } \begin{cases} m \leftarrow m-n; p \leftarrow p-r; q \leftarrow q-s; \end{cases} \\ \quad \textbf{else } \begin{cases} n \leftarrow n-m; r \leftarrow r-p; s \leftarrow s-q; \end{cases} \end{cases}$$

if $m=0$

$$\begin{cases} \textbf{then } \begin{cases} k \leftarrow n; x \leftarrow r; y \leftarrow s; \end{cases} \\ \textbf{else } \begin{cases} k \leftarrow m; x \leftarrow p; y \leftarrow q; \end{cases} \end{cases}$$

236 Clearly A and A' must have ten digits. Let $A = a_{10}a_9\ldots a_1$ be the consecutive digits of A and $A' = a'_{10}a'_9\ldots a'_1$. Now, $A+A' = 10^{10}$ if and only if there is a $j, 0 \leq j \leq 9$ for which $a_1+a'_1 = a_2+a'_2 = \cdots = a_j+a'_j = 0, a_{j+1}+a'_{j+1} = 10, a_{j+2}+a'_{j+2} = a_{j+3}+a'_{j+3} = \cdots = a_{10}+a'_{10} = 9$. Notice that $j=0$ implies that there are no sums of the form $a_{j+k}+a'_{j+k}, k \geq 2$, and $j=9$ implies that there are no sums of the form $a_l+a'_l, 1 \leq l \leq j$. On adding all these sums, we gather

$$a_1+a'_1+a_2+a'_2+\cdots+a_{10}+a'_{10} = 10+9(9-j).$$

Since the a'_s are a permutation of the a_s, we see that the sinistral side of the above equality is the even number $2(a_1+a_2+\cdots+a_{10})$. This implies that j must be odd. But this implies that $a_1+a'_1 = 0$, which gives the result.

237 We want non-negative integer solutions to the equation

$$.79x+.41y = 63.58 \implies 79x+41y = 6358.$$

Using the Euclidean Algorithm we find, successively

$$79 = 1\cdot 41+38;\quad 41 = 1\cdot 38+3;\quad 38 = 3\cdot 12+2;\quad 3 = 1\cdot 2+1.$$

Hence

$$\begin{aligned} 1 &= 3-2 \\ &= 3-(38-3\cdot 12) \\ &= -38+3\cdot 13 \\ &= -38+(41-38)\cdot 13 \\ &= 38\cdot(-14)+41\cdot 13 \\ &= (79-41)(-14)+41\cdot 13 \\ &= 79(-14)+41(27) \end{aligned}$$

A solution to $79x+41y=1$ is thus $(x,y) = (-14,27)$. Thus $79(-89012)+41(171666) = 6358$ and the parametrisation $79(-89012+41t)+41(171666-79t) = 1$ provides infinitely many solutions. We need non-negative solutions so we need, simultaneously

$$-89012+41t \geq 0 \implies t \geq 2172 \quad\wedge\quad 171666-79t \geq 0 \implies t \leq 2172.$$

Thus taking $t = 2172$ we obtain $x = -89012+41(2172) = 40$ and $y = 171666-79(2172) = 78$, and indeed $.79(40)+.41(78) = 63.58$.

238 Since $3^{100} \equiv (3^{40})^2 3^{20} \equiv 3^{20} \mod 100$, we only need to concern ourselves with the last quantity. Now (all congruences $\mod 100$)

$$3^4 \equiv 81 \implies 3^8 \equiv 81^2 \equiv 61 \implies 3^{16} \equiv 61^2 \equiv 21.$$

We deduce, as $20 = 16+4$, that

$$3^{20} \equiv 3^{16}3^4 \equiv (21)(81) \equiv 1 \mod 100,$$

and the last two digits are 01.

Chapter 6

Enumeration

6.1 The Multiplication and Sum Rules

We begin our study of combinatorial methods with the following two fundamental principles.

239 Definition (Cardinality of a Set) If S is a set, then its *cardinality* is the number of elements it has. We denote the cardinality of S by $\text{card}(S)$.

240 Rule (Sum Rule: Disjunctive Form) Let $E_1, E_2, \ldots, E_k$, be pairwise finite disjoint sets. Then

$$\text{card}(E_1 \cup E_2 \cup \cdots \cup E_k) = \text{card}(E_1) + \text{card}(E_2) + \cdots + \text{card}(E_k).$$

241 Rule (Product Rule) Let $E_1, E_2, \ldots, E_k$, be finite sets. Then

$$\text{card}(E_1 \times E_2 \times \cdots \times E_k) = \text{card}(E_1) \cdot \text{card}(E_2) \cdots \text{card}(E_k).$$

242 Example How many ordered pairs of integers (x,y) are there such that $0 < |xy| \leq 5$?

Solution: Put $E_k = \{(x,y) \in \mathbb{Z}^2 : |xy| = k\}$ for $k = 1, \ldots, 5$. Then the desired number is

$$\text{card}(E_1) + \text{card}(E_2) + \cdots + \text{card}(E_5).$$

Then

$$\begin{aligned}
E_1 &= \{(-1,-1),(-1,1),(1,-1),(1,1)\} \\
E_2 &= \{(-2,-1),(-2,1),(-1,-2),(-1,2),(1,-2),(1,2),(2,-1),(2,1)\} \\
E_3 &= \{(-3,-1),(-3,1),(-1,-3),(-1,3),(1,-3),(1,3),(3,-1),(3,1)\} \\
E_4 &= \{(-4,-1),(-4,1),(-2,-2),(-2,2),(-1,-4),(-1,4),(1,-4),(1,4),(2,-2),(2,2),(4,-1),(4,1)\} \\
E_5 &= \{(-5,-1),(-5,1),(-1,-5),(-1,5),(1,-5),(1,5),(5,-1),(5,1)\}
\end{aligned}$$

The desired number is therefore $4+8+8+12+8 = 40$.

243 Example The positive divisors of 400 are written in increasing order

$$1, 2, 4, 5, 8, \ldots, 200, 400.$$

How many integers are there in this sequence. How many of the divisors of 400 are perfect squares?

Solution: Since $400 = 2^4 \cdot 5^2$, any positive divisor of 400 has the form $2^a 5^b$ where $0 \leq a \leq 4$ and $0 \leq b \leq 2$. Thus there are 5 choices for a and 3 choices for b for a total of $5 \cdot 3 = 15$ positive divisors.

To be a perfect square, a positive divisor of 400 must be of the form $2^\alpha 5^\beta$ with $\alpha \in \{0,2,4\}$ and $\beta \in \{0,2\}$. Thus there are $3 \cdot 2 = 6$ divisors of 400 which are also perfect squares.

By arguing as in example **??**, we obtain the following theorem.

244 Theorem Let the positive integer n have the prime factorisation

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k},$$

where the p_i are different primes, and the a_i are integers ≥ 1. If $d(n)$ denotes the number of positive divisors of n, then

$$d(n) = (a_1+1)(a_2+1)\cdots(a_k+1).$$

245 Example (AHSME 1977) How many paths consisting of a sequence of horizontal and/or vertical line segments, each segment connecting a pair of adjacent letters in figure **??** spell $CONTEST$?

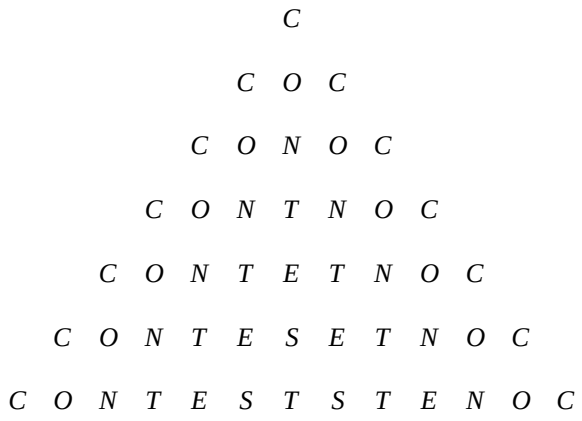

Figure 6.1: Problem **??**.

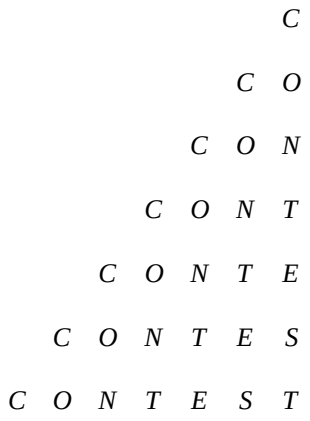

Figure 6.2: Problem **??**.

Solution: Split the diagram, as in figure **??**. Since every required path must use the bottom right T, we count paths starting from this T and reaching up to a C. Since there are six more rows that we can travel to, and since at each stage we can go either up or left, we have $2^6 = 64$ paths. The other half of the figure will provide 64 more paths. Since the middle column is shared by both halves, we have a total of $64+64-1 = 127$ paths.

246 Example The integers from 1 to 1000 are written in succession. Find the sum of all the digits.

Solution: When writing the integers from 000 to 999 (with three digits), $3 \times 1000 = 3000$ digits are used. Each of the 10 digits is used an equal number of times, so each digit is used 300 times. The the sum of the digits in the interval 000 to 999 is thus

$$(0+1+2+3+4+5+6+7+8+9)(300) = 13500.$$

Therefore, the sum of the digits when writing the integers from 1 to 1000 is $13500+1 = 13501$.

Aliter: Pair up the integers from 0 to 999 as

$$(0,999),\ (1,998),\ (2,997),\ (3,996),\ \ldots,(499,500).$$

Each pair has sum of digits 27 and there are 500 such pairs. Adding 1 for the sum of digits of 1000, the required total is

$$27 \cdot 500 + 1 = 13501.$$

247 Example The strictly positive integers are written in succession

$$1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,\ldots$$

Which digit occupies the 3000-th position?

Solution: Upon using

$$\begin{aligned} 9\cdot 1 &= 9 && \text{1-digit integers,}\\ 90\cdot 2 &= 180 && \text{2-digit integers,}\\ 900\cdot 3 &= 2700 && \text{3-digit integers,} \end{aligned}$$

a total of $9+180+2700=2889$ digits have been used, so the 3000-th digit must belong to a 4-digit integer. There remains to use $3000-2889=111$ digits, and $111=4\cdot 27+3$, so the 3000-th digit is the third digit of the 28-th 4-digit integer, that is, the third digit of 4027, namely 2.

6.2 Combinatorial Methods

Most counting problems we will be dealing with can be classified into one of four categories. We explain such categories by means of an example.

248 Example Consider the set $\{a,b,c,d\}$. Suppose we "select" two letters from these four. Depending on our interpretation, we may obtain the following answers.

❶ **Permutations with repetitions.** The *order* of listing the letters is important, and *repetition is* allowed. In this case there are $4\cdot 4=16$ possible selections:

aa	*ab*	*ac*	*ad*
ba	*bb*	*bc*	*bd*
ca	*cb*	*cc*	*cd*
da	*db*	*dc*	*dd*

❷ **Permutations without repetitions.** The *order* of listing the letters is important, and *repetition is not* allowed. In this case there are $4\cdot 3=12$ possible selections:

	ab	*ac*	*ad*
ba		*bc*	*bd*
ca	*cb*		*cd*
da	*db*	*dc*	

❸ **Combinations with repetitions.** The *order* of listing the letters is **not** important, and *repetition is* allowed. In this case there are $\frac{4\cdot 3}{2}+4=10$ possible selections:

aa	*ab*	*ac*	*ad*
	bb	*bc*	*bd*
		cc	*cd*
			dd

❹ **Combinations without repetitions.** The *order* of listing the letters is **not** important, and *repetition is not* allowed. In this case there are $\frac{4\cdot 3}{2} = 6$ possible selections:

	ab	*ac*	*ad*
		bc	*bd*
			cd

We will now consider some examples of each situation.

6.2.1 Permutations without Repetitions

249 Definition We define the symbol ! (factorial), as follows: $0! = 1$, and for integer $n \geq 1$,

$$n! = 1\cdot 2\cdot 3\cdots n.$$

$n!$ is read *n factorial*.

250 Example We have

$$\begin{aligned} 1! &= 1, \\ 2! &= 1\cdot 2 = 2, \\ 3! &= 1\cdot 2\cdot 3 = 6, \\ 4! &= 1\cdot 2\cdot 3\cdot 4 = 24, \\ 5! &= 1\cdot 2\cdot 3\cdot 4\cdot 5 = 120. \end{aligned}$$

251 Example Write a code fragment to compute $n!$.

Solution: The following is an iterative way of solving this problem.

Algorithm 6.2.1: FACTORIAL(n)

comment: *returns* $n!$

$m \leftarrow 1$

while $n > 1$

$\begin{cases} m \leftarrow n * m \\ n \leftarrow n - 1 \end{cases}$

return (m)

252 Definition Let $x_1, x_2, \ldots, x_n$ be n distinct objects. A *permutation* of these objects is simply a rearrangement of them.

253 Example There are 24 permutations of the letters in $MATH$, namely

$$\begin{array}{cccccc} MATH & MAHT & MTAH & MTHA & MHTA & MHAT \\ AMTH & AMHT & ATMH & ATHM & AHTM & AHMT \\ TAMH & TAHM & TMAH & TMHA & THMA & THAM \\ HATM & HAMT & HTAM & HTMA & HMTA & HMAT \end{array}$$

254 Theorem Let $x_1, x_2, \ldots, x_n$ be n distinct objects. Then there are $n!$ permutations of them.

Proof: *The first position can be chosen in n ways, the second object in $n-1$ ways, the third in $n-2$, etc. This gives*

$$n(n-1)(n-2)\cdots 2\cdot 1 = n!.$$

❑

255 Example Write a code fragment that prints all $n!$ of the set $\{1, 2, \ldots, n\}$.

Solution: The following programme prints them in lexicographical order. We use examples **??** and **??**.

Algorithm 6.2.2: PERMUTATIONS(n)

$k \leftarrow n-1$

while $X[k] > X[k-1]$

$\{ k \leftarrow k-1$

$t \leftarrow k+1$

while $((t < n)$ **and** $(X[t+1] > X[k]))$

$\{ t \leftarrow t+1$

comment: *now* $X[k+1] > \ldots > X[t] > X[k] > X[t+1] > \ldots > X[n]$

$Swap(X[k], X[t])$

comment: *now* $X[k+1] > \ldots > X[n]$

$ReverseArray(X[k+1], \ldots, X[n])$

256 Example A bookshelf contains 5 German books, 7 Spanish books and 8 French books. Each book is different from one another.

❶ How many different arrangements can be done of these books?

❷ How many different arrangements can be done of these books if books of each language must be next to each other?

❸ How many different arrangements can be done of these books if all the French books must be next to each other?

❹ How many different arrangements can be done of these books if no two French books must be next to each other?

Solution:

❶ We are permuting $5+7+8=20$ objects. Thus the number of arrangements sought is $20! = 2432902008176640000$.

❷ "Glue" the books by language, this will assure that books of the same language are together. We permute the 3 languages in 3! ways. We permute the German books in 5! ways, the Spanish books in 7! ways and the French books in 8! ways. Hence the total number of ways is $3!5!7!8! = 146313216000$.

❸ Align the German books and the Spanish books first. Putting these $5+7=12$ books creates $12+1=13$ spaces (we count the space before the first book, the spaces between books and the space after the last book). To assure that all the French books are next each other, we "glue" them together and put them in one of these spaces. Now, the French books can be permuted in 8! ways and the non-French books can be permuted in 12! ways. Thus the total number of permutations is

$$(13)8!12! = 251073478656000.$$

❹ Align the German books and the Spanish books first. Putting these $5+7=12$ books creates $12+1=13$ spaces (we count the space before the first book, the spaces between books and the space after the last book). To assure that no two French books are next to each other, we put them into these spaces. The first French book can be put into any of 13 spaces, the second into any of 12, etc., the eighth French book can be put into any 6 spaces. Now, the non-French books can be permuted in 12! ways. Thus the total number of permutations is

$$(13)(12)(11)(10)(9)(8)(7)(6)12!,$$

which is 24856274386944000.

257 Example Determine how many 3-digit integers written in decimal notation do not have a 0 in their decimal expansion. Also, find the sum of all these 3-digit numbers.

Solution: There are $9\cdot 9\cdot 9 = 729$ 3-digit integers not possessing a 0 in their decimal expansion. If $100x+10y+z$ is such an integer, then given for every fixed choice of a variable, there are $9\cdot 9 = 81$ choices of the other two variables. Hence the required sum is

$$81(1+2+\cdot+9)100+81(1+2+\cdot+9)10+81(1+2+\cdot+9)1 = 404595.$$

258 Example Determine how many 3-digit integers written in decimal notation possess at least one 0 in their decimal expansion. What is the sum of all these integers.

Solution: Using example **??**, there are $900-729=171$ such integers. The sum of *all* the three digit integers is

$$100+101+\cdots+998+999.$$

To obtain this sum, observe that there are 900 terms, and that you obtain the same sum adding backwards as forwards:

$$\begin{aligned} S &= 100 + 101 + \cdots + 999 \\ S &= 999 + 998 + \cdots + 100 \\ 2S &= 1099 + 1099 + \cdots + 1099 \\ &= 900(1099), \end{aligned}$$

giving $S = \dfrac{900(1099)}{2} = 494550$. The required sum is $494550 - 404595 = 89955$.

6.2.2 Permutations with Repetitions

We now consider permutations with repeated objects.

259 Example In how many ways may the letters of the word

$$MASSACHUSETTS$$

be permuted?

Solution: We put subscripts on the repeats forming

$$MA_1S_1S_2A_2CHUS_3ET_1T_2S_4.$$

There are now 13 distinguishable objects, which can be permuted in 13! different ways by Theorem **??**. For each of these 13! permutations, A_1A_2 can be permuted in 2! ways, $S_1S_2S_3S_4$ can be permuted in 4! ways, and T_1T_2 can be permuted in 2! ways. Thus the over count 13! is corrected by the total actual count

$$\frac{13!}{2!4!2!} = 64864800.$$

A reasoning analogous to the one of example **??**, we may prove

260 Theorem Let there be k types of objects: n_1 of type 1; n_2 of type 2; etc. Then the number of ways in which these $n_1+n_2+\cdots+n_k$ objects can be rearranged is

$$\frac{(n_1+n_2+\cdots+n_k)!}{n_1!n_2!\cdots n_k!}.$$

261 Example In how many ways may we permute the letters of the word *MASSACHUSETTS* in such a way that *MASS* is always together, in this order?

Solution: The particle *MASS* can be considered as one block and the 9 letters $A, C, H, U, S, E, T, T, S$. In $A, C, H, U, S, E, T, T, S$ there are four S's and two T's and so the total number of permutations sought is

$$\frac{10!}{2!2!} = 907200.$$

262 Example In how many ways may we write the number 9 as the sum of three positive integer summands? Here order counts, so, for example, $1+7+1$ is to be regarded different from $7+1+1$.

Solution: We first look for answers with

$$a+b+c = 9, 1 \leq a \leq b \leq c \leq 7$$

and we find the permutations of each triplet. We have

(a,b,c)	Number of permutations
$(1,1,7)$	$\frac{3!}{2!} = 3$
$(1,2,6)$	$3! = 6$
$(1,3,5)$	$3! = 6$
$(1,4,4)$	$\frac{3!}{2!} = 3$
$(2,2,5)$	$\frac{3!}{2!} = 3$
$(2,3,4)$	$3! = 6$
$(3,3,3)$	$\frac{3!}{3!} = 1$

Thus the number desired is

$$3+6+6+3+3+6+1 = 28.$$

263 Example In how many ways can the letters of the word **MURMUR** be arranged without letting two letters which are alike come together?

Solution: If we started with, say , **MU** then the **R** could be arranged as follows:

M	**U**	**R**		**R**	

,

M	**U**	**R**			**R**

,

M	**U**		**R**		**R**

.

In the first case there are $2! = 2$ of putting the remaining **M** and **U**, in the second there are $2! = 2$ and in the third there is only 1!. Thus starting the word with **MU** gives $2+2+1 = 5$ possible arrangements. In the general case, we can choose the first letter of the word in 3 ways, and the second in 2 ways. Thus the number of ways sought is $3 \cdot 2 \cdot 5 = 30$.

264 Example In how many ways can the letters of the word **AFFECTION** be arranged, keeping the vowels in their natural order and not letting the two **F**'s come together?

Solution: There are $\frac{9!}{2!}$ ways of permuting the letters of **AFFECTION**. The 4 vowels can be permuted in 4! ways, and in only one of these will they be in their natural order. Thus there are $\frac{9!}{2!4!}$ ways of permuting the letters of **AFFECTION** in which their vowels keep their natural order.

Now, put the 7 letters of **AFFECTION** which are not the two **F**'s. This creates 8 spaces in between them where we put the two **F**'s. This means that there are $8 \cdot 7!$ permutations of **AFFECTION** that keep the two **F**'s together. Hence there are $\frac{8 \cdot 7!}{4!}$ permutations of **AFFECTION** where the vowels occur in their natural order.

In conclusion, the number of permutations sought is

$$\frac{9!}{2!4!} - \frac{8 \cdot 7!}{4!} = \frac{8!}{4!}\left(\frac{9}{2} - 1\right) = \frac{8 \cdot 7 \cdot 6 \cdot 5 \cdot 4!}{4!} \cdot \frac{7}{2} = 5880$$

6.2.3 Combinations without Repetitions

265 Definition Let n, k be non-negative integers with $0 \leq k \leq n$. The symbol $\binom{n}{k}$ (read "*n choose k*") is defined and denoted by

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n \cdot (n-1) \cdot (n-2) \cdots (n-k+1)}{1 \cdot 2 \cdot 3 \cdots k}.$$

☞ *Observe that in the last fraction, there are k factors in both the numerator and denominator. Also, observe the boundary conditions*

$$\binom{n}{0} = \binom{n}{n} = 1, \quad \binom{n}{1} = \binom{n}{n-1} = n.$$

266 Example We have

$$\begin{aligned}
\tbinom{6}{3} &= \tfrac{6\cdot5\cdot4}{1\cdot2\cdot3} = 20, \\
\tbinom{11}{2} &= \tfrac{11\cdot10}{1\cdot2} = 55, \\
\tbinom{12}{7} &= \tfrac{12\cdot11\cdot10\cdot9\cdot8\cdot7\cdot6}{1\cdot2\cdot3\cdot4\cdot5\cdot6\cdot7} = 792, \\
\tbinom{110}{109} &= 110, \\
\tbinom{110}{0} &= 1.
\end{aligned}$$

☞ *Since $n-(n-k) = k$, we have for integer n, k, $0 \leq k \leq n$, the symmetry identity*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n!}{(n-k)!(n-(n-k))!} = \binom{n}{n-k}.$$

This can be interpreted as follows: if there are n different tickets in a hat, choosing k of them out of the hat is the same as choosing $n-k$ of them to remain in the hat.

267 Example

$$\binom{11}{9} = \binom{11}{2} = 55,$$
$$\binom{12}{5} = \binom{12}{7} = 792.$$

268 Definition Let there be n distinguishable objects. A *k-combination* is a selection of k, $(0 \leq k \leq n)$ objects from the n made without regards to order.

269 Example The 2-combinations from the list $\{X,Y,Z,W\}$ are

$$XY, XZ, XW, YZ, YW, WZ.$$

270 Example The 3-combinations from the list $\{X,Y,Z,W\}$ are

$$XYZ, XYW, XZW, YWZ.$$

271 Theorem Let there be n distinguishable objects, and let k, $0 \leq k \leq n$. Then the numbers of k-combinations of these n objects is $\binom{n}{k}$.

Proof: *Pick any of the k objects. They can be ordered in $n(n-1)(n-2)\cdots(n-k+1)$, since there are n ways of choosing the* first, $n-1$ *ways of choosing the* second, *etc. This particular choice of k objects can be permuted in $k!$ ways. Hence the total number of k-combinations is*

$$\frac{n(n-1)(n-2)\cdots(n-k+1)}{k!} = \binom{n}{k}.$$

❑

272 Example From a group of 10 people, we may choose a committee of 4 in $\binom{10}{4} = 210$ ways.

273 Example Three different integers are drawn from the set $\{1,2,\ldots,20\}$. In how many ways may they be drawn so that their sum is divisible by 3?

Solution: In $\{1,2,\ldots,20\}$ there are

6 numbers leaving remainder 0

7 numbers leaving remainder 1

7 numbers leaving remainder 2

The sum of three numbers will be divisible by 3 when (a) the three numbers are divisible by 3; (b) one of the numbers is divisible by 3, one leaves remainder 1 and the third leaves remainder 2 upon division by 3; (c) all three leave remainder 1 upon division by 3; (d) all three leave remainder 2 upon division by 3. Hence the number of ways is

$$\binom{6}{3} + \binom{6}{1}\binom{7}{1}\binom{7}{1} + \binom{7}{3} + \binom{7}{3} = 384.$$

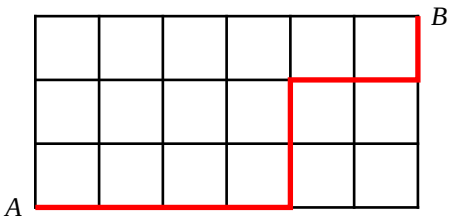

Figure 6.3: Example **??**.

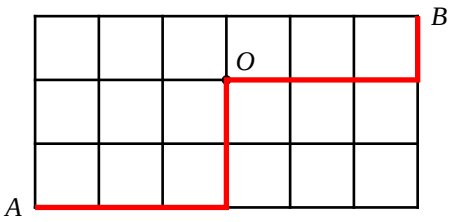

Figure 6.4: Example **??**.

274 Example To count the number of shortest routes from A to B in figure **??** observe that any shortest path must consist of 6 horizontal moves and 3 vertical ones for a total of $6+3=9$ moves. Of these 9 moves once we choose the 6 horizontal ones the 3 vertical ones are determined. Thus there are $\binom{9}{6}=84$ paths.

275 Example To count the number of shortest routes from A to B in figure **??** that pass through point O we count the number of paths from A to O (of which there are $\binom{5}{3}=20$) and the number of paths from O to B (of which there are $\binom{4}{3}=4$). Thus the desired number of paths is $\binom{5}{3}\binom{4}{3}=(20)(4)=80$.

6.2.4 Combinations with Repetitions

276 Theorem (De Moivre) Let n be a positive integer. The number of positive integer solutions to

$$x_1+x_2+\cdots+x_r=n$$

is

$$\binom{n-1}{r-1}.$$

Proof: *Write n as*

$$n=1+1+\cdots+1+1,$$

where there are n 1s and $n-1$ +s. To decompose n in r summands we only need to choose $r-1$ pluses from the $n-1$, which proves the theorem. ❑

277 Example In how many ways may we write the number 9 as the sum of three positive integer summands? Here order counts, so, for example, $1+7+1$ is to be regarded different from $7+1+1$.

Solution: Notice that this is example **??**. We are seeking integral solutions to

$$a+b+c=9,\quad a>0,b>0,c>0.$$

By Theorem **??** this is

$$\binom{9-1}{3-1}=\binom{8}{2}=28.$$

278 Example In how many ways can 100 be written as the sum of four positive integer summands?

Solution: We want the number of positive integer solutions to

$$a+b+c+d=100,$$

which by Theorem **??** is

$$\binom{99}{3}=156849.$$

279 Corollary Let n be a positive integer. The number of non-negative integer solutions to

$$y_1+y_2+\cdots+y_r=n$$

is

$$\binom{n+r-1}{r-1}.$$

Proof: *Put $x_r-1=y_r$. Then $x_r\geq 1$. The equation*

$$x_1-1+x_2-1+\cdots+x_r-1=n$$

is equivalent to

$$x_1+x_2+\cdots+x_r=n+r,$$

which from Theorem **??**, *has*

$$\binom{n+r-1}{r-1}$$

solutions. ❑

280 Example Find the number of quadruples (a,b,c,d) of integers satisfying

$$a+b+c+d=100,\ a\geq 30, b>21, c\geq 1, d\geq 1.$$

Solution: Put $a'+29=a, b'+20=b$. Then we want the number of positive integer solutions to

$$a'+29+b'+21+c+d=100,$$

or

$$a'+b'+c+d=50.$$

By Theorem **??** this number is

$$\binom{49}{3}=18424.$$

281 Example In how many ways may 1024 be written as the product of three positive integers?

Solution: Observe that $1024=2^{10}$. We need a decomposition of the form $2^{10}=2^a2^b2^c$, that is, we need integers solutions to

$$a+b+c=10,\quad a\geq 0, b\geq 0, c\geq 0.$$

By Corollary **??** there are $\binom{10+3-1}{3-1}=\binom{12}{2}=66$ such solutions.

282 Example Find the number of quadruples (a,b,c,d) of non-negative integers which satisfy the inequality

$$a+b+c+d\leq 2001.$$

Solution: The number of non-negative solutions to

$$a+b+c+d\leq 2001$$

equals the number of solutions to

$$a+b+c+d+f=2001$$

where f is a non-negative integer. This number is the same as the number of positive integer solutions to

$$a_1-1+b_1-1+c_1-1+d_1-1+f_1-1=2001,$$

which is easily seen to be $\binom{2005}{4}$.

6.3 Inclusion-Exclusion

The Sum Rule **??** gives us the cardinality for unions of finite sets that are mutually disjoint. In this section we will drop the disjointness requirement and obtain a formula for the cardinality of unions of general finite sets.

The Principle of Inclusion-Exclusion is attributed to both Sylvester and to Poincaré.

283 Theorem (Two set Inclusion-Exclusion)

$$\operatorname{card}(A\cup B)=\operatorname{card}(A)+\operatorname{card}(B)-\operatorname{card}(A\cap B)$$

Proof: *In the Venn diagram* **??**, *we mark by R_1 the number of elements which are simultaneously in both sets (i.e., in $A\cap B$), by R_2 the number of elements which are in A but not in B (i.e., in $A\setminus B$), and by R_3 the number of elements which are B but not in A (i.e., in $B\setminus A$). We have $R_1+R_2+R_3=\operatorname{card}(A\cup B)$, which proves the theorem.* ❑

284 Example Of 40 people, 28 smoke and 16 chew tobacco. It is also known that 10 both smoke and chew. How many among the 40 neither smoke nor chew?

Solution: Let A denote the set of smokers and B the set of chewers. Then

$$\operatorname{card}(A\cup B)=\operatorname{card}(A)+\operatorname{card}(B)-\operatorname{card}(A\cap B)=28+16-10=34,$$

meaning that there are 34 people that either smoke or chew (or possibly both). Therefore the number of people that neither smoke nor chew is $40-34=6$.
Aliter: We fill up the Venn diagram in figure **??** as follows. Since $|A\cap B|=8$, we put an 10 in the intersection. Then we put a $28-10=18$ in the part that A does not overlap B and a $16-10=6$ in the part of B that does not overlap A. We have accounted for $10+18+6=34$ people that are in at least one of the set. The remaining $40-34=6$ are outside the sets.

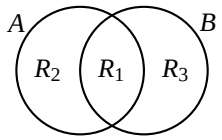

Figure 6.5: Two-set Inclusion-Exclusion

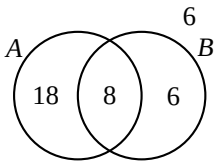

Figure 6.6: Example **??**.

285 Example Consider the set

$$A=\{2,4,6,\ldots,114\}.$$

❶ How many elements are there in A?
❷ How many are divisible by 3?
❸ How many are divisible by 5?
❹ How many are divisible by 15?
❺ How many are divisible by either 3, 5 or both?
❻ How many are neither divisible by 3 nor 5?
❼ How many are divisible by exactly one of 3 or 5?

Solution: Let $A_3\subset A$ be the set of those integers divisible by 3 and $A_5\subset A$ be the set of those integers divisible by 5.

❶ Notice that the elements are $2=2(1)$, $4=2(2)$, …, $114=2(57)$. Thus $\text{card}\,(A)=57$.
❷ There are $\lfloor\frac{57}{3}\rfloor=19$ integers in A divisible by 3. They are

$$\{6,12,18,\ldots,114\}.$$

Notice that $114=6(19)$. Thus $\text{card}\,(A_3)=19$.
❸ There are $\lfloor\frac{57}{5}\rfloor=11$ integers in A divisible by 5. They are

$$\{10,20,30,\ldots,110\}.$$

Notice that $110=10(11)$. Thus $\text{card}\,(A_5)=11$
❹ There are $\lfloor\frac{57}{15}\rfloor=3$ integers in A divisible by 15. They are $\{30,60,90\}$. Notice that $90=30(3)$. Thus $\text{card}\,(A_{15})=3$, and observe that by Theorem **??** we have $\text{card}\,(A_{15})=\text{card}\,(A_3\cap A_5)$.
❺ We want $\text{card}\,(A_3\cup A_5)=19+11=30$.
❻ We want

$$\text{card}\,(A\setminus(A_3\cup A_5))=\text{card}\,(A)-\text{card}\,(A_3\cup A_5)=57-30=27.$$

❼ We want

$$\begin{aligned}\text{card}\,((A_3\cup A_5)\setminus(A_3\cap A_5)) &= \text{card}\,((A_3\cup A_5))-\text{card}\,(A_3\cap A_5)\\ &= 30-3\\ &= 27.\end{aligned}$$

286 Example How many integers between 1 and 1000 inclusive, do not share a common factor with 1000, that is, are relatively prime to 1000?

Solution: Observe that $1000 = 2^3 5^3$, and thus from the 1000 integers we must weed out those that have a factor of 2 or of 5 in their prime factorisation. If A_2 denotes the set of those integers divisible by 2 in the interval $[1;1000]$ then clearly $\text{card}\,(A_2) = \lfloor \frac{1000}{2} \rfloor = 500$. Similarly, if A_5 denotes the set of those integers divisible by 5 then $\text{card}\,(A_5) = \lfloor \frac{1000}{5} \rfloor = 200$. Also $\text{card}\,(A_2 \cap A_5) = \lfloor \frac{1000}{10} \rfloor = 100$. This means that there are $\text{card}\,(A_2 \cup A_5) = 500 + 200 - 100 = 600$ integers in the interval $[1;1000]$ sharing at least a factor with 1000, thus there are $1000 - 600 = 400$ integers in $[1;1000]$ that do not share a factor prime factor with 1000.

We now derive a three-set version of the Principle of Inclusion-Exclusion.

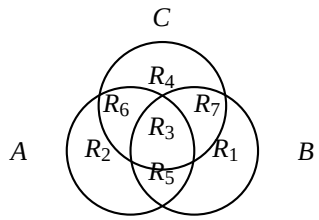

Figure 6.7: Three-set Inclusion-Exclusion

287 Theorem (Three set Inclusion-Exclusion)

$$\begin{aligned}\text{card}\,(A \cup B \cup C) &= \text{card}\,(A) + \text{card}\,(B) + \text{card}\,(C) \\ &\quad - \text{card}\,(A \cap B) - \text{card}\,(B \cap C) - \text{card}\,(C \cap A) \\ &\quad + \text{card}\,(A \cap B \cap C)\end{aligned}$$

Proof: *Using the associativity and distributivity of unions of sets, we see that*

$$\begin{aligned}\text{card}\,(A \cup B \cup C) &= \text{card}\,(A \cup (B \cup C)) \\ &= \text{card}\,(A) + \text{card}\,(B \cup C) - \text{card}\,(A \cap (B \cup C)) \\ &= \text{card}\,(A) + \text{card}\,(B \cup C) - \text{card}\,((A \cap B) \cup (A \cap C)) \\ &= \text{card}\,(A) + \text{card}\,(B) + \text{card}\,(C) - \text{card}\,(B \cap C) \\ &\quad - \text{card}\,(A \cap B) - \text{card}\,(A \cap C) \\ &\quad + \text{card}\,((A \cap B) \cap (A \cap C)) \\ &= \text{card}\,(A) + \text{card}\,(B) + \text{card}\,(C) - \text{card}\,(B \cap C) \\ &\quad - (\text{card}\,(A \cap B) + \text{card}\,(A \cap C) - \text{card}\,(A \cap B \cap C)) \\ &= \text{card}\,(A) + \text{card}\,(B) + \text{card}\,(C) \\ &\quad - \text{card}\,(A \cap B) - \text{card}\,(B \cap C) - \text{card}\,(C \cap A) \\ &\quad + \text{card}\,(A \cap B \cap C)\,.\end{aligned}$$

This gives the Inclusion-Exclusion Formula for three sets. See also figure **??**.

❑

Observe that in the Venn diagram in figure **??** there are 8 disjoint regions (the 7 that form $A \cup B \cup C$ and the outside region, devoid of any element belonging to $A \cup B \cup C$).

288 Example How many integers between 1 and 600 inclusive are not divisible by neither 3, nor 5, nor 7?

Solution: Let A_k denote the numbers in $[1;600]$ which are divisible by $k = 3,5,7$. Then

$$\begin{aligned}
\operatorname{card}(A_3) &= \lfloor \tfrac{600}{3} \rfloor = 200, \\
\operatorname{card}(A_5) &= \lfloor \tfrac{600}{5} \rfloor = 120, \\
\operatorname{card}(A_7) &= \lfloor \tfrac{600}{7} \rfloor = 85, \\
\operatorname{card}(A_{15}) &= \lfloor \tfrac{600}{15} \rfloor = 40 \\
\operatorname{card}(A_{21}) &= \lfloor \tfrac{600}{21} \rfloor = 28 \\
\operatorname{card}(A_{35}) &= \lfloor \tfrac{600}{35} \rfloor = 17 \\
\operatorname{card}(A_{105}) &= \lfloor \tfrac{600}{105} \rfloor = 5
\end{aligned}$$

By Inclusion-Exclusion there are $200+120+85-40-28-17+5 = 325$ integers in $[1;600]$ divisible by at least one of 3, 5, or 7. Those not divisible by these numbers are a total of $600-325 = 275$.

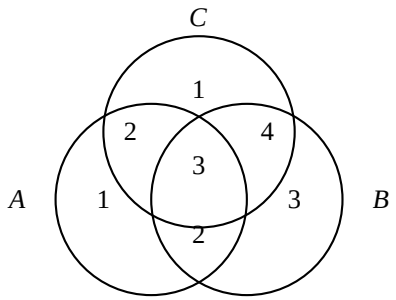

Figure 6.8: Example **??**.

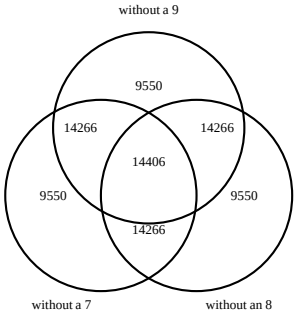

Figure 6.9: Example **??**.

289 Example In a group of 30 people, 8 speak English, 12 speak Spanish and 10 speak French. It is known that 5 speak English and Spanish, 5 Spanish and French, and 7 English and French. The number of people speaking all three languages is 3. How many do not speak any of these languages?

Solution: Let A be the set of all English speakers, B the set of Spanish speakers and C the set of French speakers in our group. We fill-up the Venn diagram in figure **??** successively. In the intersection of all three we put 8. In the region common to A and B which is not filled up we put $5-2 = 3$. In the region common to A and C which is not already filled up we put $5-3 = 2$. In the region common to B and C which is not already filled up, we put $7-3 = 4$. In the remaining part of A we put $8-2-3-2 = 1$, in the remaining part of B we put $12-4-3-2 = 3$, and in the remaining part of C we put $10-2-3-4 = 1$. Each of the mutually disjoint regions comprise a total of $1+2+3+4+1+2+3 = 16$ persons. Those outside these three sets are then $30-16 = 14$.

290 Example Consider the set of 5-digit positive integers written in decimal notation.

1. How many are there?
2. How many do not have a 9 in their decimal representation?
3. How many have at least one 9 in their decimal representation?
4. How many have exactly one 9?
5. How many have exactly two 9's?
6. How many have exactly three 9's?

7. How many have exactly four 9's?
8. How many have exactly five 9's?
9. How many have neither an 8 nor a 9 in their decimal representation?
10. How many have neither a 7, nor an 8, nor a 9 in their decimal representation?
11. How many have either a 7, an 8, or a 9 in their decimal representation?

Solution:

1. There are 9 possible choices for the first digit and 10 possible choices for the remaining digits. The number of choices is thus $9 \cdot 10^4 = 90000$.
2. There are 8 possible choices for the first digit and 9 possible choices for the remaining digits. The number of choices is thus $8 \cdot 9^4 = 52488$.
3. The difference $90000 - 52488 = 37512$.
4. We condition on the first digit. If the first digit is a 9 then the other four remaining digits must be different from 9, giving $9^4 = 6561$ such numbers. If the first digit is not a 9, then there are 8 choices for this first digit. Also, we have $\binom{4}{1} = 4$ ways of choosing where the 9 will be, and we have 9^3 ways of filling the 3 remaining spots. Thus in this case there are $8 \cdot 4 \cdot 9^3 = 23328$ such numbers. In total there are $6561 + 23328 = 29889$ five-digit positive integers with exactly one 9 in their decimal representation.
5. We condition on the first digit. If the first digit is a 9 then one of the remaining four must be a 9, and the choice of place can be accomplished in $\binom{4}{1} = 4$ ways. The other three remaining digits must be different from 9, giving $4 \cdot 9^3 = 2916$ such numbers. If the first digit is not a 9, then there are 8 choices for this first digit. Also, we have $\binom{4}{2} = 6$ ways of choosing where the two 9's will be, and we have 9^2 ways of filling the two remaining spots. Thus in this case there are $8 \cdot 6 \cdot 9^2 = 3888$ such numbers. Altogether there are $2916 + 3888 = 6804$ five-digit positive integers with exactly two 9's in their decimal representation.
6. Again we condition on the first digit. If the first digit is a 9 then two of the remaining four must be 9's, and the choice of place can be accomplished in $\binom{4}{2} = 6$ ways. The other two remaining digits must be different from 9, giving $6 \cdot 9^2 = 486$ such numbers. If the first digit is not a 9, then there are 8 choices for this first digit. Also, we have $\binom{4}{3} = 4$ ways of choosing where the three 9's will be, and we have 9 ways of filling the remaining spot. Thus in this case there are $8 \cdot 4 \cdot 9 = 288$ such numbers. Altogether there are $486 + 288 = 774$ five-digit positive integers with exactly three 9's in their decimal representation.
7. If the first digit is a 9 then three of the remaining four must be 9's, and the choice of place can be accomplished in $\binom{4}{3} = 4$ ways. The other remaining digit must be different from 9, giving $4 \cdot 9 = 36$ such numbers. If the first digit is not a 9, then there are 8 choices for this first digit. Also, we have $\binom{4}{4} = 4$ ways of choosing where the four 9's will be, thus filling all the spots. Thus in this case there are $8 \cdot 1 = 8$ such numbers. Altogether there are $36 + 8 = 44$ five-digit positive integers with exactly three 9's in their decimal representation.
8. There is obviously only 1 such positive integer.

   Observe that
   $37512 = 29889 + 6804 + 774 + 44 + 1$.
9. We have 7 choices for the first digit and 8 choices for the remaining 4 digits, giving $7 \cdot 8^4 = 28672$ such integers.
10. We have 6 choices for the first digit and 7 choices for the remaining 4 digits, giving $6 \cdot 7^4 = 14406$ such integers.
11. We use inclusion-exclusion. From figure **??**, the numbers inside the circles add up to 85854. Thus the desired number is $90000 - 85854 = 4146$.

291 Example

How many integral solutions to the equation

$$a + b + c + d = 100,$$

are there given the following constraints:

$$1 \le a \le 10,\ b \ge 0,\ c \ge 2, 20 \le d \le 30?$$

Solution: We use Inclusion-Exclusion. There are $\binom{80}{3} = 82160$ integral solutions to

$$a + b + c + d = 100,\ \ a \ge 1, b \ge 0, c \ge 2, d \ge 20.$$

Let A be the set of solutions with

$$a \ge 11, b \ge 0, c \ge 2, d \ge 20$$

and B be the set of solutions with

$$a \ge 1, b \ge 0, c \ge 2, d \ge 31.$$

Then $\text{card}\,(A) = \binom{70}{3}$, $\text{card}\,(B) = \binom{69}{3}$, $\text{card}\,(A \cap B) = \binom{59}{3}$ and so

$$\text{card}\,(A \cup B) = \binom{70}{3} + \binom{69}{3} - \binom{59}{3} = 74625.$$

The total number of solutions to

$$a + b + c + d = 100$$

with

$$1 \leq a \leq 10,\ b \geq 0,\ c \geq 2, 20 \leq d \leq 30$$

is thus

$$\binom{80}{3} - \binom{70}{3} - \binom{69}{3} + \binom{59}{3} = 7535.$$

Homework

292 Problem Telephone numbers in *Land of the Flying Camels* have 7 digits, and the only digits available are $\{0,1,2,3,4,5,7,8\}$. No telephone number may begin in 0, 1 or 5. Find the number of telephone numbers possible that meet the following criteria:

❶ You may repeat all digits.

❷ You may not repeat any of the digits.

❸ You may repeat the digits, but the phone number must be even.

❹ You may repeat the digits, but the phone number must be odd.

❺ You may not repeat the digits and the phone numbers must be odd.

293 Problem The number 3 can be expressed as a sum of one or more positive integers in four ways, namely, as 3, $1+2$, $2+1$, and $1+1+1$. Shew that any positive integer n can be so expressed in 2^{n-1} ways.

294 Problem Let $n = 2^{31}3^{19}$. How many positive integer divisors of n^2 are less than n but do not divide n?

295 Problem In how many ways can one decompose the set

$$\{1,2,3,\ldots,100\}$$

into subsets A,B,C satisfying

$$A \cup B \cup C = \{1,2,3,\ldots,100\} \quad \text{and} \quad A \cap B \cap C = \varnothing?$$

296 Problem How many two or three letter initials for people are available if at least one of the letters must be a D and one allows repetitions?

297 Problem How many strictly positive integers have all their digits distinct?

298 Problem To write a book 1890 digits were utilised. How many pages does the book have?

299 Problem The sequence of palindromes, starting with 1 is written in ascending order

$$1,2,3,4,5,6,7,8,9,11,22,33,\ldots$$

Find the 1984-th positive palindrome.

300 Problem (AIME 1994) Given a positive integer n, let $p(n)$ be the product of the non-zero digits of n. (If n has only one digit, then $p(n)$ is equal to that digit.) Let

$$S = p(1) + p(2) + \cdots + p(999).$$

Find S.

301 Problem In each of the 6-digit numbers

$$333333, 225522, 118818, 707099,$$

each digit in the number appears at least twice. Find the number of such 6-digit natural numbers.

302 Problem In each of the 7-digit numbers

$$1001011, 5550000, 3838383, 7777777,$$

each digit in the number appears at least thrice. Find the number of such 7-digit natural numbers.

303 Problem Would you believe a market investigator that reports that of 1000 people, 816 like candy, 723 like ice cream, 645 cake, while 562 like both candy and ice cream, 463 like both candy and cake, 470 both ice cream and cake, while 310 like all three? State your reasons!

304 Problem A survey shews that 90% of high-schoolers in Philadelphia like at least one of the following activities: going to the movies, playing sports, or reading. It is known that 45% like the movies, 48% like sports, and 35% like reading. Also, it is known that 12% like both the movies and reading, 20% like only the movies, and 15% only reading. What percent of high-schoolers like all three activities?

305 Problem An auto insurance company has $10,000$ policyholders. Each policy holder is classified as

- young or old,
- male or female, and
- married or single.

Of these policyholders, 3000 are young, 4600 are male, and 7000 are married. The policyholders can also be classified as 1320 young males, 3010 married males, and 1400 young married persons. Finally, 600 of the policyholders are young married males.

How many of the company's policyholders are young, female, and single?

306 Problem In *Medieval High* there are forty students. Amongst them, fourteen like Mathematics, sixteen like theology, and eleven like alchemy. It is also known that seven like Mathematics and theology, eight like theology and alchemy and five like Mathematics and alchemy. All three subjects are favoured by four students. How many students like neither Mathematics, nor theology, nor alchemy?

307 Problem (AHSME 1991) For a set S, let $n(S)$ denote the number of subsets of S. If A,B,C, are sets for which

$$n(A)+n(B)+n(C)=n(A\cup B\cup C) \text{ and } \operatorname{card}(A)=\operatorname{card}(B)=100,$$

then what is the minimum possible value of $\operatorname{card}(A\cap B\cap C)$?

308 Problem (Lewis Carroll in *A Tangled Tale.*) In a very hotly fought battle, at least 70% of the combatants lost an eye, at least 75% an ear, at least 80% an arm, and at least 85% a leg. What can be said about the percentage who lost all four members?

Answers

292 We have

❶ This is $5\cdot 8^6=1310720$.

❷ This is $5\cdot 7\cdot 6\cdot 5\cdot 4\cdot 3\cdot 2=25200$.

❸ This is $5\cdot 8^5\cdot 4=655360$.

❹ This is $5\cdot 8^5\cdot 4=655360$.

❺ We condition on the last digit. If the last digit were 1 or 5 then we would have 5 choices for the first digit, and so we would have

$$5\cdot 6\cdot 5\cdot 4\cdot 3\cdot 2\cdot 2=7200$$

phone numbers. If the last digit were either 3 or 7, then we would have 4 choices for the last digit and so we would have

$$4\cdot 6\cdot 5\cdot 4\cdot 3\cdot 2\cdot 2=5760$$

phone numbers. Thus the total number of phone numbers is

$$7200+5760=12960.$$

293 $n=\underbrace{1+1+\cdots+1}_{n-1\ +'\text{s}}$. One either erases or keeps a plus sign.

294 There are 589 such values. The easiest way to see this is to observe that there is a bijection between the divisors of n^2 which are $>n$ and those $<n$. For if $n^2=ab$, with $a>n$, then $b<n$, because otherwise $n^2=ab>n\cdot n=n^2$, a contradiction. Also, there is exactly one decomposition $n^2=n\cdot n$. Thus the desired number is

$$\lfloor\!\lfloor \frac{d(n^2)}{2} \rfloor\!\rfloor +1-d(n)=\lfloor\!\lfloor \frac{(63)(39)}{2} \rfloor\!\rfloor +1-(32)(20)=589.$$

295 The conditions of the problem stipulate that both the region outside the circles in diagram **??** and R_3 will be empty. We are thus left with 6 regions to distribute 100 numbers. To each of the 100 numbers we may thus assign one of 6 labels. The number of sets thus required is 6^{100}.

296 $(26^2-25^2)+(26^3-25^3)=2002$

297

$$\begin{aligned}
&9+9\cdot 9\\
&\quad +9\cdot 9\cdot 8+9\cdot 9\cdot 8\cdot 7\\
&\quad +9\cdot 9\cdot 8\cdot 7\cdot 6+9\cdot 9\cdot 8\cdot 7\cdot 6\cdot 5\\
&\quad +9\cdot 9\cdot 8\cdot 7\cdot 6\cdot 5\cdot 4+9\cdot 9\cdot 8\cdot 7\cdot 6\cdot 5\cdot 4\cdot 3\\
&\quad +9\cdot 9\cdot 8\cdot 7\cdot 6\cdot 5\cdot 4\cdot 3\cdot 2\\
&\quad +9\cdot 9\cdot 8\cdot 7\cdot 6\cdot 5\cdot 4\cdot 3\cdot 2\cdot 1\\
&\quad =8877690
\end{aligned}$$

298 A total of

$$1\cdot 9+2\cdot 90=189$$

digits are used to write pages 1 to 99, inclusive. We have of $1890-189=1701$ digits at our disposition which is enough for $1701/3=567$ extra pages (starting from page 100). The book has $99+567=666$ pages.

299 It is easy to see that there are 9 palindromes of 1-digit, 9 palindromes with 2-digits, 90 with 3-digits, 90 with 4-digits, 900 with 5-digits and 900 with 6-digits. The last palindrome with 6 digits, 999999, constitutes the $9+9+90+90+900+900=1998$th palindrome. Hence, the 1997th palindrome is 998899, the 1996th palindrome is 997799, the 1995th palindrome is 996699, the 1994th is 995599, etc., until we find the 1984th palindrome to be 985589.

300 If $x=0$, put $m(x)=1$, otherwise put $m(x)=x$. We use three digits to label all the integers, from 000 to 999 If a,b,c are digits, then clearly $p(100a+10b+c)=m(a)m(b)m(c)$. Thus

$$p(000)+\cdots+p(999)=m(0)m(0)m(0)+\cdots+m(9)m(9)m(9),$$

which in turn

$$\begin{aligned}
&=(m(0)+m(1)+\cdots+m(9))^3\\
&=(1+1+2+\cdots+9)^3\\
&=46^3\\
&=97336.
\end{aligned}$$

Hence

$$\begin{aligned}
S&=p(001)+p(002)+\cdots+p(999)\\
&=97336-p(000)\\
&=97336-m(0)m(0)m(0)\\
&=97335.
\end{aligned}$$

301 The numbers belong to the following categories: (I) all six digits are identical; (II) there are exactly two different digits used, three of one kind, three of the other; (III) there are exactly two different digits used, two of one kind, four of the other; (IV) there are exactly three different digits used, two of each kind.

There are clearly 9 numbers belonging to category (I). To count the numbers in the remaining categories, we must consider the cases when the digit 0 is used or not. If 0 is not used, then there are $\binom{9}{2}\cdot\dfrac{6!}{3!3!}=720$ integers in category (II); $\binom{9}{1}\binom{8}{1}\cdot\dfrac{6!}{2!4!}=1080$ integers in category

(III); and $\binom{9}{3}\cdot\frac{6!}{2!2!2!}=7560$ integers in category (IV). If 0 is used, then the integers may not start with 0. There are $\binom{9}{1}\cdot\frac{5!}{2!3!}=90$ in category (II) ; $\binom{9}{1}\cdot(\frac{5!}{1!4!}+\frac{5!}{3!2!})=135$ in category (III) ; and $\binom{9}{2}\cdot 2\cdot\frac{5!}{1!2!2!}=3240$ in category (IV). Thus there are altogether

$$9+720+1080+7560+90+135+3240=12834$$

such integers.

302 The numbers belong to the following categories: (I) all seven digits are identical; (II) there are exactly two different digits used, three of one kind, four of the other.

There are clearly 9 numbers belonging to category (I). To count the numbers in the remaining category (II), we must consider the cases when the digit 0 is used or not. If 0 is not used, then there are $\binom{9}{1}\binom{8}{1}\cdot\frac{7!}{3!4!}=2520$ integers in category (II). If 0 is used, then the integers may not start with 0. There are $\binom{9}{1}\cdot\frac{6!}{2!4!}+\binom{9}{1}\cdot\frac{6!}{3!3!}=315$ in category (II). Thus there are altogether $2520+315+9=2844$ such integers.

303 Let C denote the set of people who like candy, I the set of people who like ice cream, and K denote the set of people who like cake. We are given that $\text{card}\,(C)=816$, $\text{card}\,(I)=723$, $\text{card}\,(K)=645$, $\text{card}\,(C\cap I)=562$, $\text{card}\,(C\cap K)=463$, $\text{card}\,(I\cap K)=470$, and $\text{card}\,(C\cap I\cap K)=310$. By Inclusion-Exclusion we have

$$\begin{aligned}\text{card}\,(C\cup I\cup K) &= \text{card}\,(C)+\text{card}\,(I)+\text{card}\,(K)\\ &\quad -\text{card}\,(C\cap I)-\text{card}\,(C\cap K)-\text{card}\,(I\cap C)\\ &\quad +\text{card}\,(C\cap I\cap K)\\ &= 816+723+645-562-463-470+310\\ &= 999.\end{aligned}$$

The investigator miscounted, or probably did not report one person who may not have liked any of the three things.

304 We make the Venn diagram in as in figure **??**. From it we gather the following system of equations

$$\begin{array}{rcrcrcrcrcrcl}
x & + & y & + & z & & & & & + & 20 & = & 45\\
x & & & + & z & + & t & + & u & & & = & 48\\
x & + & y & & & + & t & & & + & 15 & = & 35\\
x & + & y & & & & & & & & & = & 12\\
x & + & y & + & z & + & t & + & u & + & 15 & + & 20 \quad = \quad 90
\end{array}$$

The solution of this system is seen to be $x=5$, $y=7$, $z=13$, $t=8$, $u=22$. Thus the percent wanted is 5%.

305 Let Y,F,S,M stand for young, female, single, male, respectively, and let Ma stand for married. We have

$$\begin{aligned}\text{card}\,(Y\cap F\cap S) &= \text{card}\,(Y\cap F)-\text{card}\,(Y\cap F\cap Ma)\\ &= \text{card}\,(Y)-\text{card}\,(Y\cap M)\\ &\quad -(\text{card}\,(Y\cap Ma)-\text{card}\,(Y\cap Ma\cap M))\\ &= 3000-1320-(1400-600)\\ &= 880.\end{aligned}$$

306 Let A be the set of students liking Mathematics, B the set of students liking theology, and C be the set of students liking alchemy. We are given that

$$\text{card}\,(A) = 14, \text{card}\,(B) = 16, \text{card}\,(C) = 11, \text{card}\,(A \cap B) = 7, \text{card}\,(B \cap C) = 8, \text{card}\,(A \cap C) = 5,$$

and

$$\text{card}\,(A \cap B \cap C) = 4.$$

By the Principle of Inclusion-Exclusion,

$$\text{card}\left(\complement A \cap \complement B \cap \complement C\right) = 40 - \text{card}\,(A) - \text{card}\,(B) - \text{card}\,(C) + \text{card}\,(A \cap B) + \text{card}\,(A \cap C) + \text{card}\,(B \cap C) - \text{card}\,(A \cap B \cap C)$$

Substituting the numerical values of these cardinalities

$$40 - 14 - 16 - 11 + 7 + 5 + 8 - 4 = 15.$$

307 A set with k elements has 2^k different subsets. We are given

$$2^{100} + 2^{100} + 2^{\text{card}(C)} = 2^{\text{card}(A \cup B \cup C)}.$$

This forces $\text{card}\,(C) = 101$, as $1 + 2^{\text{card}(C)-101}$ is larger than 1 and a power of 2. Hence $\text{card}\,(A \cup B \cup C) = 102$. Using the Principle Inclusion-Exclusion, since $\text{card}\,(A) + \text{card}\,(B) + \text{card}\,(C) - \text{card}\,(A \cup B \cup C) = 199$,

$$\begin{aligned}
\text{card}\,(A \cap B \cap C) &= \text{card}\,(A \cap B) + \text{card}\,(A \cap C) + \text{card}\,(B \cap C) - 199 \\
&= (\text{card}\,(A) + \text{card}\,(B) - \text{card}\,(A \cup B)) + (\text{card}\,(A) + \text{card}\,(C) - \text{card}\,(A \cup C)) \\
&\quad + (\text{card}\,(B) + \text{card}\,(C) - \text{card}\,(B \cup C)) - 199 \\
&= 403 - \text{card}\,(A \cup B) - \text{card}\,(A \cup C) - \text{card}\,(B \cup C).
\end{aligned}$$

As $A \cup B, A \cup C, B \cup C \subseteq A \cup B \cup C$, the cardinalities of all these sets are ≤ 102. Thus

$$\text{card}\,(A \cap B \cap C) = 403 - \text{card}\,(A \cup B) - \text{card}\,(A \cup C) - \text{card}\,(B \cup C) \geq 403 - 3 \cdot 102 = 97.$$

The example

$$A = \{1, 2, \ldots, 100\}, B = \{3, 4, \ldots, 102\},$$

and

$$C = \{1, 2, 3, 4, 5, 6, \ldots, 101, 102\}$$

shews that $\text{card}\,(A \cap B \cap C) = \text{card}\,(\{4, 5, 6, \ldots, 100\}) = 97$ is attainable.

308 Let A denote the set of those who lost an eye, B denote those who lost an ear, C denote those who lost an arm and D denote those losing a leg. Suppose there are n combatants. Then

$$\begin{aligned}
n &\geq \text{card}\,(A \cup B) \\
&= \text{card}\,(A) + \text{card}\,(B) - \text{card}\,(A \cap B) \\
&= .7n + .75n - \text{card}\,(A \cap B),
\end{aligned}$$

$$\begin{aligned}
n &\geq \text{card}\,(C \cup D) \\
&= \text{card}\,(C) + \text{card}\,(D) - \text{card}\,(C \cap D) \\
&= .8n + .85n - \text{card}\,(C \cap D).
\end{aligned}$$

This gives

$$\begin{aligned}
\text{card}\,(A \cap B) &\geq .45n, \\
\text{card}\,(C \cap D) &\geq .65n.
\end{aligned}$$

This means that

$$\begin{aligned}
n &\geq \text{card}\,((A \cap B) \cup (C \cap D)) \\
&= \text{card}\,(A \cap B) + \text{card}\,(C \cap D) - \text{card}\,(A \cap B \cap C \cap D) \\
&\geq .45n + .65n - \text{card}\,(A \cap B \cap C \cap D),
\end{aligned}$$

whence

$$\text{card}\,(A\cap B\cap C\cap D)\geq .45+.65n-n=.1n.$$

This means that at least 10% of the combatants lost all four members.

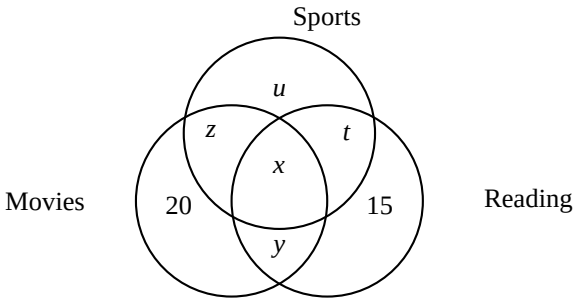

Figure 6.10: Problem **??**.

Chapter 7

Sums and Recursions

7.1 Famous Sums

To obtain a closed form for

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

we utilise Gauss' trick: If

$$A_n=1+2+3+\cdots+n$$

then

$$A_n=n+(n-1)+\cdots+1.$$

Adding these two quantities,

$$\begin{array}{rcccccccc} A_n & = & 1 & + & 2 & + & \cdots & + & n \\ A_n & = & n & + & (n-1) & + & \cdots & + & 1 \\ 2A_n & = & (n+1) & + & (n+1) & + & \cdots & + & (n+1) \\ & = & n(n+1), & & & & & & \end{array}$$

since there are n summands. This gives $A_n=\frac{n(n+1)}{2}$, that is,

$$1+2+\cdots+n=\frac{n(n+1)}{2}. \tag{7.1}$$

Applying Gauss's trick to the general arithmetic sum

$$(a)+(a+d)+(a+2d)+\cdots+(a+(n-1)d)$$

we obtain

$$(a)+(a+d)+(a+2d)+\cdots+(a+(n-1)d)=\frac{n(2a+(n-1)d)}{2} \tag{7.2}$$

309 Example Each element of the set $\{10,11,12,\ldots,19,20\}$ is multiplied by each element of the set $\{21,22,23,\ldots,29,30\}$. If all these products are added, what is the resulting sum?

Solution: This is asking for the product $(10+11+\cdots+20)(21+22+\cdots+30)$ after all the terms are multiplied. But

$$10+11+\cdots+20=\frac{(20+10)(11)}{2}=165$$

and

$$21+22+\cdots+30=\frac{(30+21)(10)}{2}=255.$$

The required total is $(165)(255)=42075$.

310 Example Find the sum of all integers between 1 and 100 that leave remainder 2 upon division by 6.

Solution: We want the sum of the integers of the form $6r+2, r=0,1,\ldots,16$. But this is

$$\sum_{r=0}^{16}(6r+2)=6\sum_{r=0}^{16}r+\sum_{r=0}^{16}2=6\frac{16(17)}{2}+2(17)=850.$$

A *geometric progression* is one of the form

$$a, ar, ar^2, ar^3, \ldots, ar^{n-1}, \ldots,$$

311 Example Find the following geometric sum:

$$1+2+4+\cdots+1024.$$

Solution: Let

$$S=1+2+4+\cdots+1024.$$

Then

$$2S=2+4+8+\cdots+1024+2048.$$

Hence

$$S=2S-S=(2+4+8\cdots+2048)-(1+2+4+\cdots+1024)=2048-1=2047.$$

312 Example Find the geometric sum

$$x=\frac{1}{3}+\frac{1}{3^2}+\frac{1}{3^3}+\cdots+\frac{1}{3^{99}}.$$

Solution: We have

$$\frac{1}{3}x=\frac{1}{3^2}+\frac{1}{3^3}+\cdots+\frac{1}{3^{99}}+\frac{1}{3^{100}}.$$

Then

$$\begin{aligned}\tfrac{2}{3}x &= x-\tfrac{1}{3}x\\ &= (\tfrac{1}{3}+\tfrac{1}{3^2}+\tfrac{1}{3^3}+\cdots+\tfrac{1}{3^{99}})\\ &\qquad -(\tfrac{1}{3^2}+\tfrac{1}{3^3}+\cdots+\tfrac{1}{3^{99}}+\tfrac{1}{3^{100}})\\ &= \tfrac{1}{3}-\tfrac{1}{3^{100}}.\end{aligned}$$

From which we gather

$$x=\frac{1}{2}-\frac{1}{2\cdot 3^{99}}.$$

Let us sum now the geometric series

$$S=a+ar+ar^2+\cdots+ar^{n-1}.$$

Plainly, if $r=1$ then $S=na$, so we may assume that $r\neq 1$. We have

$$rS=ar+ar^2+\cdots+ar^n.$$

Hence

$$S-rS=a+ar+ar^2+\cdots+ar^{n-1}-ar-ar^2-\cdots-ar^n=a-ar^n.$$

From this we deduce that

$$S=\frac{a-ar^n}{1-r},$$

that is,

$$a+ar+\cdots+ar^{n-1}=\frac{a-ar^n}{1-r} \tag{7.3}$$

If $|r|<1$ then $r^n\to 0$ as $n\to\infty$.
For $|r|<1$, we obtain the sum of the infinite geometric series

$$a+ar+ar^2+\cdots=\frac{a}{1-r} \tag{7.4}$$

313 Example A fly starts at the origin and goes 1 unit up, $1/2$ unit right, $1/4$ unit down, $1/8$ unit left, $1/16$ unit up, etc., *ad infinitum.* In what coordinates does it end up?

Solution: Its x coordinate is

$$\frac{1}{2}-\frac{1}{8}+\frac{1}{32}-\cdots=\frac{\frac{1}{2}}{1-\frac{-1}{4}}=\frac{2}{5}.$$

Its y coordinate is

$$1-\frac{1}{4}+\frac{1}{16}-\cdots=\frac{1}{1-\frac{-1}{4}}=\frac{4}{5}.$$

Therefore, the fly ends up in $(\frac{2}{5},\frac{4}{5})$.

We now sum again of the first n positive integers, which we have already computed using Gauss' trick.

314 Example Find a closed formula for

$$A_n=1+2+\cdots+n.$$

Solution: Observe that

$$k^2-(k-1)^2=2k-1.$$

From this

$$\begin{aligned}
1^2-0^2 &= 2\cdot 1-1\\
2^2-1^2 &= 2\cdot 2-1\\
3^2-2^2 &= 2\cdot 3-1\\
\vdots &\quad \vdots\ \ \vdots\\
n^2-(n-1)^2 &= 2\cdot n-1
\end{aligned}$$

Adding both columns,

$$n^2-0^2=2(1+2+3+\cdots+n)-n.$$

Solving for the sum,

$$1+2+3+\cdots+n=n^2/2+n/2=\frac{n(n+1)}{2}.$$

315 Example Find the sum

$$1^2+2^2+3^2+\cdots+n^2.$$

Solution: Observe that

$$k^3-(k-1)^3=3k^2-3k+1.$$

Hence

$$\begin{aligned}
1^3-0^3 &= 3\cdot 1^2-3\cdot 1+1\\
2^3-1^3 &= 3\cdot 2^2-3\cdot 2+1\\
3^3-2^3 &= 3\cdot 3^2-3\cdot 3+1\\
\vdots &\quad \vdots\ \ \vdots\\
n^3-(n-1)^3 &= 3\cdot n^2-3\cdot n+1
\end{aligned}$$

Adding both columns,

$$n^3-0^3=3(1^2+2^2+3^2+\cdots+n^2)-3(1+2+3+\cdots+n)+n.$$

From the preceding example $1+2+3+\cdots+n=\cdot n^2/2+n/2=\frac{n(n+1)}{2}$ so

$$n^3-0^3=3(1^2+2^2+3^2+\cdots+n^2)-\frac{3}{2}\cdot n(n+1)+n.$$

Solving for the sum,

$$1^2+2^2+3^2+\cdots+n^2=\frac{n^3}{3}+\frac{1}{2}\cdot n(n+1)-\frac{n}{3}.$$

After simplifying we obtain

$$1^2+2^2+3^2+\cdots+n^2=\frac{n(n+1)(2n+1)}{6} \tag{7.5}$$

316 Example Add the series

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\cdots+\frac{1}{99\cdot 100}.$$

Solution: Observe that

$$\frac{1}{k(k+1)}=\frac{1}{k}-\frac{1}{k+1}.$$

Thus

$$\begin{array}{ccc}\frac{1}{1\cdot 2} & = & \frac{1}{1}-\frac{1}{2}\\ \frac{1}{2\cdot 3} & = & \frac{1}{2}-\frac{1}{3}\\ \frac{1}{3\cdot 4} & = & \frac{1}{3}-\frac{1}{4}\\ \vdots & \vdots & \vdots\\ \frac{1}{99\cdot 100} & = & \frac{1}{99}-\frac{1}{100}\end{array}$$

Adding both columns,

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\cdots+\frac{1}{99\cdot 100}=1-\frac{1}{100}=\frac{99}{100}.$$

317 Example Add

$$\frac{1}{1\cdot 4}+\frac{1}{4\cdot 7}+\frac{1}{7\cdot 10}+\cdots+\frac{1}{31\cdot 34}.$$

Solution: Observe that

$$\frac{1}{(3n+1)\cdot(3n+4)}=\frac{1}{3}\cdot\frac{1}{3n+1}-\frac{1}{3}\cdot\frac{1}{3n+4}.$$

Thus

$$\begin{array}{ccc}\frac{1}{1\cdot 4} & = & \frac{1}{3}-\frac{1}{12}\\ \frac{1}{4\cdot 7} & = & \frac{1}{12}-\frac{1}{21}\\ \frac{1}{7\cdot 10} & = & \frac{1}{21}-\frac{1}{30}\\ \frac{1}{10\cdot 13} & = & \frac{1}{30}-\frac{1}{39}\\ \vdots & \vdots & \vdots\\ \frac{1}{34\cdot 37} & = & \frac{1}{102}-\frac{1}{111}\end{array}$$

Summing both columns,

$$\frac{1}{1\cdot 4}+\frac{1}{4\cdot 7}+\frac{1}{7\cdot 10}+\cdots+\frac{1}{31\cdot 34}=\frac{1}{3}-\frac{1}{111}=\frac{12}{37}.$$

318 Example Sum

$$\frac{1}{1\cdot 4\cdot 7}+\frac{1}{4\cdot 7\cdot 10}+\frac{1}{7\cdot 10\cdot 13}+\cdots+\frac{1}{25\cdot 28\cdot 31}.$$

Solution: Observe that

$$\frac{1}{(3n+1)\cdot(3n+4)\cdot(3n+7)}=\frac{1}{6}\cdot\frac{1}{(3n+1)(3n+4)}-\frac{1}{6}\cdot\frac{1}{(3n+4)(3n+7)}.$$

Therefore

$$\begin{aligned}
\tfrac{1}{1\cdot4\cdot7} &= \tfrac{1}{6\cdot1\cdot4} - \tfrac{1}{6\cdot4\cdot7} \\
\tfrac{1}{4\cdot7\cdot10} &= \tfrac{1}{6\cdot4\cdot7} - \tfrac{1}{6\cdot7\cdot10} \\
\tfrac{1}{7\cdot10\cdot13} &= \tfrac{1}{6\cdot7\cdot10} - \tfrac{1}{6\cdot10\cdot13} \\
\vdots &\quad \vdots \quad \vdots \\
\tfrac{1}{25\cdot28\cdot31} &= \tfrac{1}{6\cdot25\cdot28} - \tfrac{1}{6\cdot28\cdot31}
\end{aligned}$$

Adding each column,

$$\frac{1}{1\cdot4\cdot7}+\frac{1}{4\cdot7\cdot10}+\frac{1}{7\cdot10\cdot13}+\cdots+\frac{1}{25\cdot28\cdot31}=\frac{1}{6\cdot1\cdot4}-\frac{1}{6\cdot28\cdot31}=\frac{9}{217}.$$

319 Example Find the sum

$$1\cdot2+2\cdot3+3\cdot4+\cdots+99\cdot100.$$

Solution: Observe that

$$k(k+1)=\frac{1}{3}(k)(k+1)(k+2)-\frac{1}{3}(k-1)(k)(k+1).$$

Therefore

$$\begin{aligned}
1\cdot2 &= \tfrac{1}{3}\cdot1\cdot2\cdot3-\tfrac{1}{3}\cdot0\cdot1\cdot2 \\
2\cdot3 &= \tfrac{1}{3}\cdot2\cdot3\cdot4-\tfrac{1}{3}\cdot1\cdot2\cdot3 \\
3\cdot4 &= \tfrac{1}{3}\cdot3\cdot4\cdot5-\tfrac{1}{3}\cdot2\cdot3\cdot4 \\
\vdots &\quad \vdots \quad \vdots \\
99\cdot100 &= \tfrac{1}{3}\cdot99\cdot100\cdot101-\tfrac{1}{3}\cdot98\cdot99\cdot100
\end{aligned}$$

Adding each column,

$$1\cdot2+2\cdot3+3\cdot4+\cdots+99\cdot100=\frac{1}{3}\cdot99\cdot100\cdot101-\frac{1}{3}\cdot0\cdot1\cdot2=333300.$$

7.2 First Order Recursions

The *order* of the recurrence is the difference between the highest and the lowest subscripts. For example

$$u_{n+2}-u_{n+1}=2$$

is of the first order, and

$$u_{n+4}+9u_n^2=n^5$$

is of the fourth order.

A recurrence is *linear* if the subscripted letters appear only to the first power. For example

$$u_{n+2}-u_{n+1}=2$$

is a linear recurrence and

$$x_n^2+nx_{n-1}=1 \text{ and } x_n+2^{x_{n-1}}=3$$

are not linear recurrences.

A recursion is *homogeneous* if all its terms contain the subscripted variable to the same power. Thus

$$x_{m+3}+8x_{m+2}-9x_m=0$$

is homogeneous. The equation

$$x_{m+3}+8x_{m+2}-9x_m=m^2-3$$

is not homogeneous.

A *closed form* of a recurrence is a formula that permits us to find the n-th term of the recurrence without having to know a priori the terms preceding it.

We outline a method for solving first order linear recurrence relations of the form

$$x_n = ax_{n-1} + f(n), a \neq 1,$$

where f is a polynomial.

1. First solve the homogeneous recurrence $x_n = ax_{n-1}$ by "raising the subscripts" in the form $x^n = ax^{n-1}$. This we call the *characteristic equation*. Cancelling this gives $x = a$. The solution to the homogeneous equation $x_n = ax_{n-1}$ will be of the form $x_n = Aa^n$, where A is a constant to be determined.
2. Test a solution of the form $x_n = Aa^n + g(n)$, where g is a polynomial of the same degree as f.

320 Example Let $x_0 = 7$ and $x_n = 2x_{n-1}, n \geq 1$. Find a closed form for x_n.

Solution: Raising subscripts we have the characteristic equation $x^n = 2x^{n-1}$. Cancelling, $x = 2$. Thus we try a solution of the form $x_n = A2^n$, were A is a constant. But $7 = x_0 = A2^0$ and so $A = 7$. The solution is thus $x_n = 7(2)^n$.
Aliter: We have

$$\begin{aligned} x_0 &= 7 \\ x_1 &= 2x_0 \\ x_2 &= 2x_1 \\ x_3 &= 2x_2 \\ \vdots &\ \vdots \ \vdots \\ x_n &= 2x_{n-1} \end{aligned}$$

Multiplying both columns,

$$x_0 x_1 \cdots x_n = 7 \cdot 2^n x_0 x_1 x_2 \cdots x_{n-1}.$$

Cancelling the common factors on both sides of the equality,

$$x_n = 7 \cdot 2^n.$$

321 Example Let $x_0 = 7$ and $x_n = 2x_{n-1} + 1, n \geq 1$. Find a closed form for x_n.

Solution: By raising the subscripts in the homogeneous equation we obtain $x^n = 2x^{n-1}$ or $x = 2$. A solution to the homogeneous equation will be of the form $x_n = A(2)^n$. Now $f(n) = 1$ is a polynomial of degree 0 (a constant) and so we test a particular constant solution C. The general solution will have the form $x_n = A2^n + B$. Now, $7 = x_0 = A2^0 + B = A + B$. Also, $x_1 = 2x_0 + 7 = 15$ and so $15 = x_1 = 2A + B$. Solving the simultaneous equations

$$\begin{aligned} A + B &= 7, \\ 2A + B &= 15, \end{aligned}$$

we find $A = 8, B = -1$. So the solution is $x_n = 8(2^n) - 1 = 2^{n+3} - 1$.
Aliter: We have:

$$\begin{aligned} x_0 &= 7 \\ x_1 &= 2x_0 + 1 \\ x_2 &= 2x_1 + 1 \\ x_3 &= 2x_2 + 1 \\ \vdots &\ \vdots \ \vdots \\ x_{n-1} &= 2x_{n-2} + 1 \\ x_n &= 2x_{n-1} + 1 \end{aligned}$$

Multiply the kth row by 2^{n-k}. We obtain

$$\begin{aligned} 2^n x_0 &= 2^n \cdot 7 \\ 2^{n-1}x_1 &= 2^n x_0 + 2^{n-1} \\ 2^{n-2}x_2 &= 2^{n-1}x_1 + 2^{n-2} \\ 2^{n-3}x_3 &= 2^{n-2}x_2 + 2^{n-3} \\ \vdots &\quad \vdots \quad \vdots \\ 2^2 x_{n-2} &= 2^3 x_{n-3} + 2^2 \\ 2x_{n-1} &= 2^2 x_{n-2} + 2 \\ x_n &= 2x_{n-1} + 1 \end{aligned}$$

Adding both columns, cancelling, and adding the geometric sum,

$$x_n = 7 \cdot 2^n + (1 + 2 + 2^2 + \cdots + 2^{n-1}) = 7 \cdot 2^n + 2^n - 1 = 2^{n+3} - 1.$$

Aliter: Let $u_n = x_n + 1 = 2x_{n-1} + 2 = 2(x_{n-1} + 1) = 2u_{n-1}$. We solve the recursion $u_n = 2u_{n-1}$ as we did on our first example: $u_n = 2^n u_0 = 2^n(x_0 + 1) = 2^n \cdot 8 = 2^{n+3}$. Finally, $x_n = u_n - 1 = 2^{n+3} - 1$.

322 Example Let $x_0 = 2, x_n = 9x_{n-1} - 56n + 63$. Find a closed form for this recursion.

Solution: By raising the subscripts in the homogeneous equation we obtain the characteristic equation $x^n = 9x^{n-1}$ or $x = 9$. A solution to the homogeneous equation will be of the form $x_n = A(9)^n$. Now $f(n) = -56n + 63$ is a polynomial of degree 1 and so we test a particular solution of the form $Bn + C$. The general solution will have the form $x_n = A9^n + Bn + C$. Now $x_0 = 2, x_1 = 9(2) - 56 + 63 = 25, x_2 = 9(25) - 56(2) + 63 = 176$. We thus solve the system

$$2 = A + C,$$

$$25 = 9A + B + C,$$

$$176 = 81A + 2B + C.$$

We find $A = 2, B = 7, C = 0$. The general solution is $x_n = 2(9^n) + 7n$.

323 Example Let $x_0 = 1, x_n = 3x_{n-1} - 2n^2 + 6n - 3$. Find a closed form for this recursion.

Solution: By raising the subscripts in the homogeneous equation we obtain the characteristic equation $x^n = 3x^{n-1}$ or $x = 9$. A solution to the homogeneous equation will be of the form $x_n = A(3)^n$. Now $f(n) = -2n^2 + 6n - 3$ is a polynomial of degree 2 and so we test a particular solution of the form $Bn^2 + Cn + D$. The general solution will have the form $x_n = A3^n + Bn^2 + Cn + D$. Now $x_0 = 1, x_1 = 3(1) - 2 + 6 - 3 = 4, x_2 = 3(4) - 2(2)^2 + 6(2) - 3 = 13, x_3 = 3(13) - 2(3)^2 + 6(3) - 3 = 36$. We thus solve the system

$$1 = A + D,$$

$$4 = 3A + B + C + D,$$

$$13 = 9A + 4B + 2C + D,$$

$$36 = 27A + 9B + 3C + D.$$

We find $A = B = 1, C = D = 0$. The general solution is $x_n = 3^n + n^2$.

324 Example Find a closed form for $x_n = 2x_{n-1} + 3^{n-1}, x_0 = 2$.

Solution: We test a solution of the form $x_n = A2^n + B3^n$. Then $x_0 = 2, x_1 = 2(2) + 3^0 = 5$. We solve the system

$$2 = A + B,$$

$$7 = 2A + 3B.$$

We find $A = 1, B = 1$. The general solution is $x_n = 2^n + 3^n$.

We now tackle the case when $a = 1$. In this case, we simply consider a polynomial g of degree 1 higher than the degree of f.

325 Example Let $x_0 = 7$ and $x_n = x_{n-1} + n, n \geq 1$. Find a closed formula for x_n.

Solution: By raising the subscripts in the homogeneous equation we obtain the characteristic equation $x^n = x^{n-1}$ or $x = 1$. A solution to the homogeneous equation will be of the form $x_n = A(1)^n = A$, a constant. Now $f(n) = n$ is a polynomial of degree 1 and so we test a particular solution of the form $Bn^2 + Cn + D$, one more degree than that of f. The general solution will have the form $x_n = A + Bn^2 + Cn + D$. Since A and D are constants, we may combine them to obtain $x_n = Bn^2 + Cn + E$. Now, $x_0 = 7, x_1 = 7 + 1 = 8, x_2 = 8 + 2 = 10$. So we solve the system

$$\begin{aligned} 7 &= E, \\ 8 &= B + C + E, \\ 10 &= 4B + 2C + E. \end{aligned}$$

We find $B = C = \frac{1}{2}, E = 7$. The general solution is $x_n = \frac{n^2}{2} + \frac{n}{2} + 7$.
Aliter: We have

$$\begin{aligned} x_0 &= 7 \\ x_1 &= x_0 + 1 \\ x_2 &= x_1 + 2 \\ x_3 &= x_2 + 3 \\ &\vdots \\ x_n &= x_{n-1} + n \end{aligned}$$

Adding both columns,

$$x_0 + x_1 + x_2 + \cdots + x_n = 7 + x_0 + x_2 + \cdots + x_{n-1} + (1 + 2 + 3 + \cdots + n).$$

Cancelling and using the fact that $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$,

$$x_n = 7 + \frac{n(n+1)}{2}.$$

Some non-linear first order recursions maybe reduced to a linear first order recursion by a suitable transformation.

326 Example A recursion satisfies $u_0 = 3, u_{n+1}^2 = u_n, n \geq 1$. Find a closed form for this recursion.

Solution: Let $v_n = \log u_n$. Then $v_n = \log u_n = \log u_{n-1}^{1/2} = \frac{1}{2} \log u_{n-1} = \frac{v_{n-1}}{2}$. As $v_n = v_{n-1}/2$, we have $v_n = v_0/2^n$, that is, $\log u_n = (\log u_0)/2^n$. Therefore, $u_n = 3^{1/2^n}$.

327 Example (Putnam 1985) Let d be a real number. For each integer $m \geq 0$, define a sequence $a_m(j), j = 0, 1, 2, \cdots$ by $a_m(0) = \frac{d}{2^m}$, and $a_m(j+1) = (a_m(j+1))^2 + 2a_m(j), j \geq 0$. Evaluate

$$\lim_{n \to \infty} a_n(n).$$

Solution: Observe that $a_m(j+1) + 1 = (a_m(j))^2 + 2a_m(j) + 1 = (a_m(j) + 1)^2$. Put $v_j = a_m(j) + 1$. Then $v_{j+1} = v_j^2$, and $\ln v_{j+1} = 2 \ln v_j$; Put $y_j = \ln v_j$. Then $y_{j+1} = 2y_j$; and hence $2^n y_0 = y_n$ or $2^n \ln v_0 = \ln v_n$ or $v_n = (v_0)^{2^n} = (1 + \frac{d}{2^m})^{2^n}$ or $a_m(n) + 1 = (1 + \frac{d}{2^m})^{2^n}$. Thus $a_n(n) = (\frac{d}{2^n} + 1)^{2^n} - 1 \to e^d - 1$ as $n \to \infty$.

7.3 Second Order Recursions

All the recursions that we have so far examined are first order recursions, that is, we find the next term of the sequence given the preceding one. Let us now briefly examine how to solve some second order recursions.

We now outline a method for solving second order homogeneous linear recurrence relations of the form

$$x_n = ax_{n-1} + bx_{n-2}.$$

1. Find the characteristic equation by "raising the subscripts" in the form $x^n = ax^{n-1} + bx^{n-2}$. Cancelling this gives $x^2 - ax - b = 0$. This equation has two roots r_1 and r_2.
2. If the roots are different, the solution will be of the form $x_n = A(r_1)^n + B(r_2)^n$, where A, B are constants.
3. If the roots are identical, the solution will be of the form $x_n = A(r_1)^n + Bn(r_1)^n$.

328 Example Let $x_0 = 1, x_1 = -1, x_{n+2} + 5x_{n+1} + 6x_n = 0$.

Solution: The characteristic equation is $x^2 + 5x + 6 = (x+3)(x+2) = 0$. Thus we test a solution of the form $x_n = A(-2)^n + B(-3)^n$. Since $1 = x_0 = A + B, -1 = -2A - 3B$, we quickly find $A = 2, B = -1$. Thus the solution is $x_n = 2(-2)^n - (-3)^n$.

329 Example Find a closed form for the Fibonacci recursion $f_0 = 0, f_1 = 1, f_n = f_{n-1} + f_{n-2}$.

Solution: The characteristic equation is $f^2 - f - 1 = 0$, whence a solution will have the form

$$f_n = A\left(\frac{1+\sqrt{5}}{2}\right)^n + B\left(\frac{1-\sqrt{5}}{2}\right)^n.$$

The initial conditions give

$$0 = A + B,$$
$$1 = A\left(\frac{1+\sqrt{5}}{2}\right) + B\left(\frac{1-\sqrt{5}}{2}\right) = \frac{1}{2}(A+B) + \frac{\sqrt{5}}{2}(A-B) = \frac{\sqrt{5}}{2}(A-B)$$

This gives $A = \frac{1}{\sqrt{5}}, B = -\frac{1}{\sqrt{5}}$. We thus have the *Cauchy-Binet Formula:*

$$f_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n \tag{7.6}$$

330 Example Solve the recursion $x_0 = 1, x_1 = 4, x_n = 4x_{n-1} - 4x_{n-2} = 0$.

Solution: The characteristic equation is $x^2 - 4x + 4 = (x-2)^2 = 0$. There is a multiple root and so we must test a solution of the form $x_n = A2^n + Bn2^n$. The initial conditions give

$$1 = A,$$
$$4 = 2A + 2B.$$

This solves to $A = 1, B = 1$. The solution is thus $x_n = 2^n + n2^n$.

7.4 Applications of Recursions

331 Example Find the recurrence relation for the number of n digit binary sequences with no pair of consecutive 1's.

Solution: It is quite easy to see that $a_1 = 2, a_2 = 3$. To form $a_n, n \geq 3$, we condition on the last digit. If it is 0, the number of sequences sought is a_{n-1}. If it is 1, the penultimate digit must be 0, and the number of sequences sought is a_{n-2}. Thus

$$a_n = a_{n-1} + a_{n-2}, a_1 = 2,\ a_2 = 3.$$

332 Example Let there be drawn n ovals on the plane. If an oval intersects each of the other ovals at exactly two points and no three ovals intersect at the same point, find a recurrence relation for the number of regions into which the plane is divided.

Solution: Let this number be a_n. Plainly $a_1 = 2$. After the $n-1$th stage, the nth oval intersects the previous ovals at $2(n-1)$ points, i.e. the nth oval is divided into $2(n-1)$ arcs. This adds $2(n-1)$ regions to the a_{n-1} previously existing. Thus

$$a_n = a_{n-1} + 2(n-1),\ a_1 = 2.$$

333 Example Find a recurrence relation for the number of regions into which the plane is divided by n straight lines if every pair of lines intersect, but no three lines intersect.

Solution: Let a_n be this number. Clearly $a_1 = 2$. The nth line is cut by he previous $n-1$ lines at $n-1$ points, adding n new regions to the previously existing a_{n-1}. Hence

$$a_n = a_{n-1} + n,\ a_1 = 2.$$

334 Example *(Derangements)* An absent-minded secretary is filling n envelopes with n letters. Find a recursion for the number D_n of ways in which she never stuffs the right letter into the right envelope.

Solution: Number the envelopes $1,2,3,\cdots,n$. We condition on the last envelope. Two events might happen. Either n and $r(1 \leq r \leq n-1)$ trade places or they do not.
In the first case, the two letters r and n are misplaced. Our task is just to misplace the other $n-2$ letters, $(1,2,\cdots,r-1,r+1,\cdots,n-1)$ in the slots $(1,2,\cdots,r-1,r+1,\cdots,n-1)$. This can be done in D_{n-2} ways. Since r can be chosen in $n-1$ ways, the first case can happen in $(n-1)D_{n-2}$ ways.
In the second case, let us say that letter r, $(1 \leq r \leq n-1)$ moves to the n-th position but n moves not to the r-th position. Since r has been misplaced, we can just ignore it. Since n is not going to the r-th position, we may relabel n as r. We now have $n-1$ numbers to misplace, and this can be done in D_{n-1} ways.
As r can be chosen in $n-1$ ways, the total number of ways for the second case is $(n-1)D_{n-1}$. Thus $D_n = (n-1)D_{n-2} + (n-1)D_{n-1}$.

335 Example There are two urns, one is full of water and the other is empty. On the first stage, half of the contains of urn I is passed into urn II. On the second stage 1/3 of the contains of urn II is passed into urn I. On stage three, 1/4 of the contains of urn I is passed into urn II. On stage four 1/5 of the contains of urn II is passed into urn I, and so on. What fraction of water remains in urn I after the 1978th stage?

Solution: Let $x_n, y_n, n = 0,1,2,\ldots$ denote the fraction of water in urns I and II respectively at stage n. Observe that $x_n + y_n = 1$ and that

$$x_0 = 1; y_0 = 0$$

$$x_1 = x_0 - \tfrac{1}{2}x_0 = \tfrac{1}{2}; y_1 = y_1 + \tfrac{1}{2}x_0 = \tfrac{1}{2}$$

$$x_2 = x_1 + \tfrac{1}{3}y_1 = \tfrac{2}{3}; y_2 = y_1 - \tfrac{1}{3}y_1 = \tfrac{1}{3}$$

$$x_3 = x_2 - \tfrac{1}{4}x_2 = \tfrac{1}{2}; y_1 = y_1 + \tfrac{1}{4}x_2 = \tfrac{1}{2}$$

$$x_4 = x_3 + \tfrac{1}{5}y_3 = \tfrac{3}{5}; y_1 = y_1 - \tfrac{1}{5}y_3 = \tfrac{2}{5}$$

$$x_5 = x_4 - \tfrac{1}{6}x_4 = \tfrac{1}{2}; y_1 = y_1 + \tfrac{1}{6}x_4 = \tfrac{1}{2}$$

$$x_6 = x_5 + \tfrac{1}{7}y_5 = \tfrac{4}{7}; y_1 = y_1 - \tfrac{1}{7}y_5 = \tfrac{3}{7}$$

$$x_7 = x_6 - \tfrac{1}{8}x_6 = \tfrac{1}{2}; y_1 = y_1 + \tfrac{1}{8}x_6 = \tfrac{1}{2}$$

$$x_8 = x_7 + \tfrac{1}{9}y_7 = \tfrac{5}{9}; y_1 = y_1 - \tfrac{1}{9}y_7 = \tfrac{4}{9}$$

A pattern emerges (which may be proved by induction) that at each odd stage n we have $x_n = y_n = \frac{1}{2}$ and that at each even stage we have (if $n = 2k$) $x_{2k} = \frac{k+1}{2k+1}, y_{2k} = \frac{k}{2k+1}$. Since $\frac{1978}{2} = 989$ we have $x_{1978} = \frac{990}{1979}$.

Homework

336 Problem Find the sum of all the integers from 1 to 1000 inclusive, which are not multiples of 3 or 5.

337 Problem The sum of a certain number of consecutive positive integers is 1000. Find these integers. (There is more than one solution. You must find them all.)

338 Problem Use the identity

$$n^5 - (n-1)^5 = 5n^4 - 10n^3 + 10n^2 - 5n + 1.$$

and the sums

$$s_1 = 1+2+\cdots+n = \frac{n(n+1)}{2},$$
$$s_2 = 1^2+2^2+\cdots+n^2 = \frac{n(n+1)(2n+1)}{6},$$
$$s_3 = 1^3+2^3+\cdots+n^3 = \left(\frac{n(n+1)}{2}\right)^2,$$

in order to find

$$s_4 = 1^4+2^4+\cdots+n^4.$$

339 Problem Find the exact value of

$$\frac{1}{1\cdot3\cdot5}+\frac{1}{3\cdot5\cdot7}+\cdots+\frac{1}{997\cdot999\cdot1001}.$$

Answers

336 We compute the sum of all integers from 1 to 1000 and weed out the sum of the multiples of 3 and the sum of the multiples of 5, but put back the multiples of 15, which we have counted twice. Put

$$A_n = 1+2+3+\cdots+n,$$
$$B = 3+6+9+\cdots+999 = 3A_{333},$$
$$C = 5+10+15+\cdots+1000 = 5A_{200},$$
$$D = 15+30+45+\cdots+990 = 15A_{66}.$$

The desired sum is

$$\begin{aligned} A_{1000}-B-C+D &= A_{1000}-3A_{333}-5A_{200}+15A_{66} \\ &= 500500-3\cdot55611-5\cdot20100+15\cdot2211 \\ &= 266332. \end{aligned}$$

337 Let the the sum of integers be $S=(l+1)+(l+2)+(l+n)$. Using Gauss' trick we obtain $S=\frac{n(2l+n+1)}{2}$. As $S=1000$, $2000=n(2l+n+1)$. Now $2000=n^2+2ln+n>n^2$, whence $n\le\lfloor\sqrt{2000}\rfloor=44$. Moreover, n and $2l+n+1$ are divisors of 2000 and are of opposite parity. Since $2000=2^4\cdot5^3$, the odd factors of 2000 are 1, 5, 25, and 125. We then see that the problem has the following solutions:

$$n=1,\ l=999,$$
$$n=5,\ l=197,$$
$$n=16,\ l=54,$$
$$n=25,\ l=27.$$

338 Using the identity for $n=1$ to n:

$$n^5 = 5s_4-10s_3+10s_2-5s_1+n,$$

whence

$$\begin{aligned} s_4 &= \frac{n^5}{5}+2s_3-2s_2+s_1-\frac{n}{5} \\ &= \frac{n^5}{5}+\frac{n^2(n+1)^2}{2}-\frac{n(n+1)(2n+1)}{3}+\frac{n(n+1)}{2}-\frac{n}{5} \\ &= \frac{n^5}{5}+\frac{n^4}{2}+\frac{n^3}{3}-\frac{n}{30}. \end{aligned}$$

339 Observe that

$$\frac{1}{(2n-1)(2n+1)}-\frac{1}{(2n+1)(2n+3)}=\frac{4}{(2n-1)(2n+1)(2n+3)}.$$

Letting $n=1$ to $n=499$ we deduce that

$$\frac{4}{1\cdot3\cdot5}+\frac{4}{3\cdot5\cdot7}+\cdots+\frac{4}{997\cdot999\cdot1001}=\frac{1}{1\cdot3}-\frac{1}{999\cdot1001},$$

whence the desired sum is

$$\frac{1}{4\cdot1\cdot3}-\frac{1}{4\cdot999\cdot1001}=\frac{83333}{999999}.$$

Chapter 8

Graph Theory

8.1 Simple Graphs

340 Definition A *simple graph (network)* $G = (V, E)$ consists of a non-empty set V (called the *vertex (node)* set) and a set E (possibly empty) of unordered pairs of elements (called the *edges* or *arcs*) of V.

Vertices are usually represented by means of dots on the plane, and the edges by means of lines connecting these dots. See figures **??** through **??** for some examples of graphs.

341 Definition If v and v' are vertices of a graph G which are joined by an edge e, we say that v is *adjacent* to v' and that v and v' are *neighbours*, and we write $e = vv'$. We say that vertex v is *incident* with an edge e if v is an endpoint of e. In this case we also say that e is incident with v.

Figure 8.1: A graph with $\operatorname{card}(V) = 1$ and $\operatorname{card}(E) = 0$.

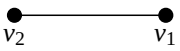

Figure 8.2: A graph with $\operatorname{card}(V) = 2$ and $\operatorname{card}(E) = 1$.

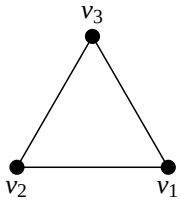

Figure 8.3: A graph with $\operatorname{card}(V) = 3$ and $\operatorname{card}(E) = 3$.

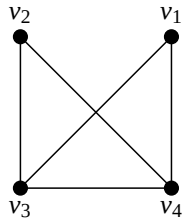

Figure 8.4: A graph with $\operatorname{card}(V) = 3$ and $\operatorname{card}(E) = 5$.

342 Definition The *degree* of a vertex is the number of edges incident to it.

Depending on whether $\operatorname{card}(V)$ is finite or not, the graph is finite or infinite. In these notes we will only consider finite graphs.

Our definition of a graph does not allow that two vertices be joined by more than one edge. If this were allowed we would obtain a *multigraph*. Neither does it allow *loops* , which are edges incident to only one vertex. A graph with loops is a *pseudograph*.

343 Definition The complete graph with n vertices K_n is the graph where any two vertices are adjacent. Thus K_n has $\binom{n}{2}$ edges.

Figure **??** shews K_1, figure **??** shews K_2, figure **??** shews K_3, and figure **??** shews K_4, figure **??** shews K_5.

344 Definition Let $G=(V,E)$ be a graph. A subset $S\subseteq V$ is an *independent set* of vertices if $uv\notin E$ for all u,v in S (S may be empty). A *bipartite graph* with bipartition X,Y is a graph such that $V=X\cup Y$, $X\cap Y=\varnothing$, and X and Y are independent sets. X and Y are called the *parts* of the bipartition.

345 Definition $K_{m,n}$ denotes the *complete bipartite graph* with $m+n$ vertices. One part, with m vertices, is connected to every other vertex of the other part, with n vertices.

346 Definition A $u-v$ *walk* in a graph $G=(V,E)$ is an alternating sequence of vertices and edges in G with starting vertex u and ending vertex v such that every edge joins the vertices immediately preceding it and immediately following it.

347 Definition A $u-v$ *trail* in a graph $G=(V,E)$ is a $u-v$ walk that does not repeat an edge, while a $u-v$ *path* is a walk that which does not repeat any vertex.

348 Definition P_n denotes a *path* of length n. It is a graph with n edges, and $n+1$ vertices $v_0v_1\cdots v_n$, where v_i is adjacent to v_{i+1} for $n=0,1,\ldots,n-1$.

349 Definition C_n denotes a *cycle* of length n. It is a graph with n edges, and n vertices $v_1\cdots v_n$, where v_i is adjacent to v_{i+1} for $n=1,\ldots,n-1$, and v_1 is adjacent to v_n.

350 Definition Q_n denotes the *n-dimensional cube*. It is a simple graph with 2^n vertices, which we label with n-tuples of 0's and 1's. Vertices of Q_n are connected by an edge if and only if they differ by exactly one coordinate. Observe that Q_n has $n2^{n-1}$ edges.

Figure **??** shews $K_{3,3}$, figure **??** shews P_3, figure **??** shews C_5, figure **??** shews Q_2, and figure **??** shews Q_3.

351 Definition A *subgraph* $G_1=(V_1,E_1)$ of a graph $G=(V,E)$ is a graph with $V_1\subseteq V$ and $E_1\subseteq E$.

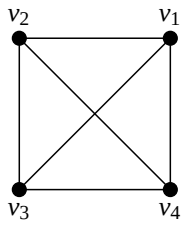

Figure 8.5: K_4.

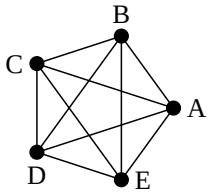

Figure 8.6: K_5.

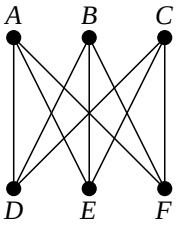

Figure 8.7: $K_{3,3}$.

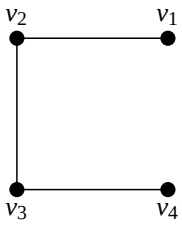

Figure 8.8: P_3.

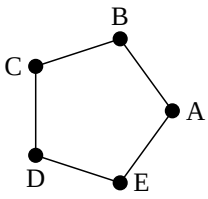

Figure 8.9: C_5.

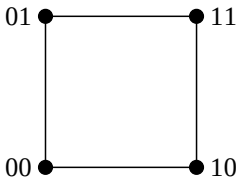

Figure 8.10: Q_2.

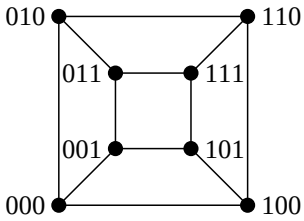

Figure 8.11: Q_3.

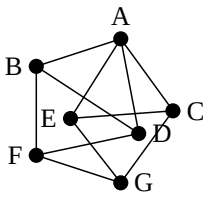

Figure 8.12: Example **??**.

We will now give a few examples of problems whose solutions become simpler when using a graph-theoretic model.

352 Example If the points of the plane are coloured with three different colours, red, white, and blue, say, shew that there will always exist two points of the same colour which are 1 unit apart.

Solution: In figure **??** all the edges have length 1. Assume the property does not hold and that A is coloured red, B is coloured white, D coloured blue. Then F must both be coloured red. Since E and C must not be red, we also conclude that G is red. But then F and G are at distance 1 apart and both coloured red which contradicts our assumption that the property did not hold.

353 Example A wolf, a goat, and a cabbage are on one bank of a river. The ferryman wants to take them across, but his boat is too small to accommodate more than one of them. Evidently, he can neither leave the wolf and the goat, or the cabbage and the goat behind. Can the ferryman still get all of them across the river?

Solution: Represent the position of a single item by 0 for one bank of the river and 1 for the other bank. The position of the three items can now be given as an ordered triplet, say (W,G,C). For example, $(0,0,0)$ means that the three items are on one bank of the river, $(1,0,0)$ means that the wolf is on one bank of the river while the goat and the cabbage are on the other bank. The object of the puzzle is now seen to be to move from $(0,0,0)$ to $(1,1,1)$, that is, traversing Q_3 while avoiding certain edges. One answer is

$$000 \to 010 \to 011 \to 001 \to 101 \to 111.$$

This means that the ferryman (i) takes the goat across, (ii) returns and that the lettuce over bringing back the goat, (iii) takes the wolf over, (iv) returns and takes the goat over. Another one is

$$000 \to 010 \to 110 \to 100 \to 101 \to 111.$$

This means that the ferryman (i) takes the goat across, (ii) returns and that the wolf over bringing back the goat, (iii) takes the lettuce over, (iv) returns and takes the goat over. The graph depicting both answers can be seen in figure **??**. You may want to visit

`http://www.cut-the-knot.org/ctk/GoatCabbageWolf.shtml`

for a pictorial representation.

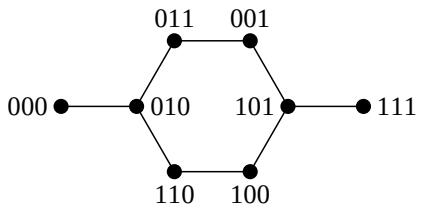

Figure 8.13: Example **??**.

354 Example (Eötvös Mathematical Competition, 1947) Prove that amongst six people in a room there are at least three who know one another, or at least three who do not know one another.

Solution: In graph-theoretic terms, we need to shew that every colouring of the edges of K_6 into two different colours, say red and blue, contains a monochromatic triangle (that is, the edges of the triangle have all the same colour). Consider an arbitrary person of this group (call him Peter). There are five other people, and of these, either three of them know Peter or else, three of them do not know Peter. Let us assume three do know Peter, as the alternative is argued similarly. If two of these three people know one another, then we have a triangle (Peter and these two, see figure **??**, where the acquaintances are marked by solid lines). If no two of these three people know one another, then we have three mutual strangers, giving another triangle (see figure **??**).

355 Example Mr. and Mrs. Landau invite four other married couples for dinner. Some people shook hands with some others, and the following rules were noted: (i) a person did not shake hands with himself, (ii) no one shook hands with his spouse, (iii) no one shook hands more than once with the same person. After the introductions, Mr. Landau asks the nine people how many hands they shook. Each of the nine people asked gives a different number. How many hands did Mrs. Landau shake?

Solution: The given numbers can either be $0,1,2,\ldots,8$, or $1,2,\ldots,9$. Now, the sequence $1,2,\ldots,9$ must be ruled out, since if a person shook hands nine times, then he must have shaken hands with his spouse, which is not allowed. The only permissible sequence is thus $0,1,2,\ldots,8$.

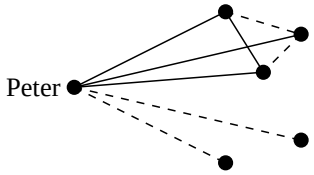

Figure 8.14: Example **??**.

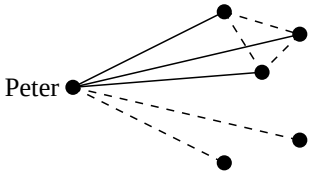

Figure 8.15: Example **??**.

Consider the person who shook hands 8 times, as in figure **??**. Discounting himself and his spouse, he must have shaken hands with everybody else. This means that he is married to the person who shook 0 hands! We now consider the person that shook 7 hands, as in figure **??**. He didn't shake hands with himself, his spouse, or with the person that shook 0 hands. But the person that shook hands only once did so with the person shaking 8 hands. Thus the person that shook hand 7 times is married to the person that shook hands once. Continuing this argument, we see the following pairs $(8,0)$, $(7,1)$, $(6,2)$, $(5,3)$. This leaves the person that shook hands 4 times without a partner, meaning that this person's partner did not give a number, hence this person must be Mrs. Landau! Conclusion: Mrs. Landau shook hands four times. A graph of the situation appears in figure **??**.

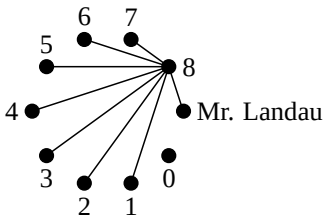

Figure 8.16: Example **??**.

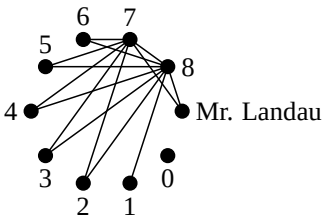

Figure 8.17: Example **??**.

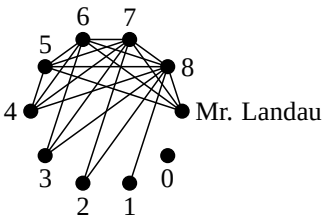

Figure 8.18: Example **??**.

8.2 Graphic Sequences

356 Definition A sequence of non-negative integers is *graphic* if there exists a graph whose degree sequence is precisely that sequence.

357 Example The sequence $1,1,1$ is graphic, since K_3 is a graph with this degree sequence, and in general, so is the sequence $\underbrace{n,n,\ldots,n}_{n+1\ n\text{'s}}$, since K_{n+1} has this degree sequence. The degree sequence $1,\underbrace{2,2,\ldots,2}_{n\text{ twos}},1$ is graphic, since P_{n+1} has this sequence. The degree sequence $\underbrace{2,2,\ldots,2}_{n\text{ twos}}$ is graphic, since C_n has this sequence. From example **??**, the sequence $0,1,2,3,4,5,6,7,8$ is graphic, whereas the sequence $1,2,3,4,5,6,7,8,9$ is not.

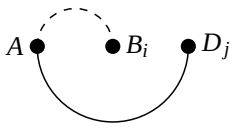

Figure 8.19: Theorem **??**.

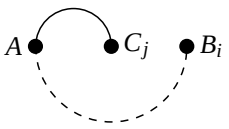

Figure 8.20: Theorem **??**.

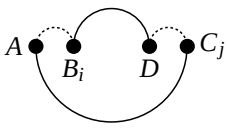

Figure 8.21: Theorem **??**.

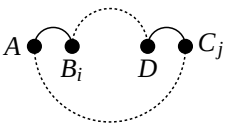

Figure 8.22: Theorem **??**.

358 Theorem (Havel-Hakimi) The two degree sequences

$$I: \quad a \geq b_1 \geq b_2 \geq \cdots \geq b_a \geq c_1 \geq c_2 \geq \cdots \geq c_n,$$

$$II: \quad b_1-1, b_2-1, \cdots, b_a-1, c_1, c_2, \cdots, c_n,$$

are simultaneously graphic.

Proof: *Assume first that the sequence II is graphic. There is a graph G' with degree sequence equal to sequence II. We construct the graph G from G' by adding a vertex and connecting it to the vertices whose degrees are $b_1-1, b_2-1, \cdots, b_a-1$. Then G is a graph whose degree sequence is sequence I, and so II $\implies$ I.*

*Assume now that sequence I is graphic. Let A, B_i, C_i be vertices with $\deg A = a, \deg B_i = b_i$, and $\deg C_i = c_i$, respectively. If A were adjacent to all the B_i, our task is finished by simply removing A. So assume that there is B_i to which A is not adjacent, and a C_j to which A is adjacent. As the sequence is arranged in decreasing order, we must have $b_i \geq c_j$. If it happens that $b_i = c_j$, we then simply exchange B_i and D_j (see figures **??** and **??**). If $b_i > c_j$ then B_i has at least one more neighbour than C_j. Call this neighbour D. In this case we remove the edges AC_j and B_iD and add the edges AB_i and DC_j to obtain a new graph with the same degree sequence as II. See figures **??** and **??**. This process is iterated until A is adjacent to all the B_i. This finishes the proof.* ❑

359 Example Determine whether the degree sequence $6,5,4,3,2,2,2,2$ is graphic.

Solution: Using the Havel-Hakimi Theorem successively we have

$$6,5,4,3,2,2,2,2 \rightarrow$$

$$4,3,2,1,1,1,2 \rightarrow$$

$$4,3,2,2,1,1,1 \rightarrow$$

$$2,1,1,0,1,1 \rightarrow$$

$$2,1,1,1,1,0 \rightarrow$$

$$0,0,1,1,0 \rightarrow$$

$$1,1,0,0,0.$$

This last sequence is graphic. By the Havel-Hakimi Theorem, the original sequence is graphic.

8.3 Connectivity

360 Definition A graph $G = (V,E)$ is *connected* if for any two of its vertices there is a path connecting them.

361 Definition A graph is *connected if for any two vertices there is a path with these vertices at its ends. A* component of a graph is a maximal connected subgraph.

362 Definition A *forest* is a graph with no cycles (acyclic). A *tree* is a connected acyclic graph. A *spanning tree* of a graph of a connected graph G is a subgraph of G which is a tree and having exactly the same of vertices as G.

8.4 Traversability

We start with the following, which is valid not only for simple graphs, but also for multigraphs and pseudographs.

363 Theorem (Handshake Lemma) Let $G = (V,E)$ be a graph. Then

$$\sum_{v \in V} \deg v = 2\text{card}\,(E)\,.$$

Proof: *If the edge connects two distinct vertices, as sum traverses through the vertices, each edge is counted twice. If the edge is a loop, then every vertex having a loop contributes 2 to the sum. This gives the theorem.* ❑

364 Corollary Every graph has an even number of vertices of odd degree.

Proof: *The sum of an odd number of odd numbers is odd. Since the sum of the degrees of the vertices in a simple graph is always even, one cannot have an odd number of odd degree vertices.* ❑

365 Definition A *trail* is a walk where all the edges are distinct. An *Eulerian trail* on a graph G is a trail that traverses every edge of G. A *tour* of G is a closed walk that traverses each edge of G at least once. An *Euler tour* on G is a tour traversing each edge of G exactly once, that is, a closed Euler trail. A graph is *eulerian* if it contains an Euler tour.

366 Theorem A nonempty connected graph is eulerian if and only if has no vertices of odd degree.

Proof: *Assume first that G is eulerian, and let C be an Euler tour of C starting and ending at vertex u. Each time a vertex v is encountered along C, two of the edges incident to v are accounted for. Since C contains every edge of G, $d(v)$ is then even for all $v \neq u$. Also, since C begins and ends in u, $d(u)$ must also be even.*

Conversely, assume that G is a connected noneulerian graph with at least one edge and no vertices of odd degree. Let W be the longest walk in G that traverses every edge at most once:

$$W = v_0, v_0v_1, v_1, v_1v_2, v_2, \ldots, v_{n-1}, v_{n-1}v_n, v_n.$$

Then W must traverse every edge incident to v_n, otherwise, W could be extended into a longer walk. In particular, W traverses two of these edges each time it passes through v_n and traverses $v_{n-1}v_n$ at the end of the walk. This accounts for an odd number of edges, but the degree of v_n is even by assumption. Hence, W must also begin at v_n, that is, $v_0 = v_n$. If W were not an Euler tour, we could find an edge not in W but incident to some vertex in W since G is connected. Call this edge uv_i. But then we can construct a longer walk:

$$u, uv_i, v_i, v_iv_{i+1}, \ldots, v_{n-1}v_n, v_n, v_0v_1, \ldots, v_{i-1}v_i, v_i.$$

This contradicts the definition of W, so W must be an Euler tour. ❑

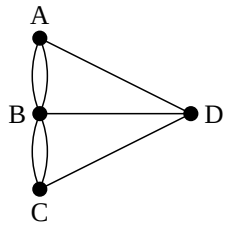

Figure 8.23: Example **??**.

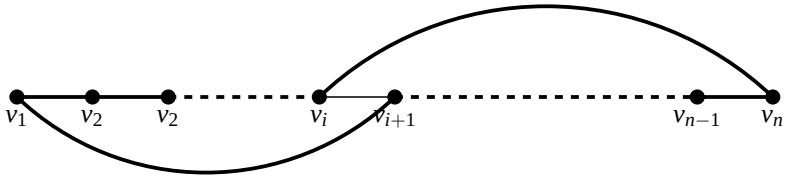

Figure 8.24: Theorem **??**

The following problem is perhaps the originator of graph theory.

367 Example (Königsberg Bridge Problem) The town of Königsberg (now called Kaliningrad) was built on an island in the Pregel River. The island sat near where two branches of the river join, and the borders of the town spreaded over to the banks of the river as well as a nearby promontory. Between these four land masses, seven bridges had been erected. The townsfolk used to amuse themselves by crossing over the bridges and asked whether it was possible to find a trail starting and ending in the same location allowing one to traverse each of the bridges exactly once. Figure **??** has a graph theoretic model of the town, with the seven edges of the graph representing the seven bridges. By Theorem **??**, this graph is not Eulerian so it is impossible to find a trail as the townsfolk asked.

368 Definition A *Hamiltonian cycle* in a graph is a cycle passing through every vertex. G is *Hamiltonian* if it contains a Hamiltonian cycle.

Unlike Theorem **??**, there is no simple characterisation of all graphs with a Hamiltonian cycle. We have the following one way result, however.

369 Theorem (Dirac's Theorem, 1952) Let $G = (V, E)$ be a graph with $n = \text{card}\,(E) \geq 3$ edges whose every vertex has degree $\geq \frac{n}{2}$. Then G is Hamiltonian.

Proof: *Arguing by contradiction, suppose G is a maximal non-Hamiltonian with with $n \geq 3$, and that G has more than 3 vertices. Then G cannot be complete. Let a and b be two non-adjacent vertices of G. By definition of G, $G + ab$ is Hamiltonian, and each of its Hamiltonian cycles must contain the edge ab. Hence, there is a Hamiltonian path $v_1v_2 \ldots v_n$ in G beginning at $v_1 = a$ and ending at $v_n = b$. Put*

$$S = \{v_i : av_{i+1} \in E\} \qquad \text{and} \qquad \{v_j : v_jb \in E\}.$$

As $v_n \in S \cap T$ we must have $\text{card}\,(S \cup T) = n$*. Moreover,* $S \cap T = \varnothing$*, since if* $v_i \S \cap T$ *then G would have the Hamiltonian cycle*

$$v_1 v_2 \cdots v_i v_n v_{n-1} \cdots v_{i+1} v_1,$$

as in figure **??***, contrary to the assumption that G is non-Hamiltonian. But then*

$$d(a) + d(b) = \text{card}\,(S) + \text{card}\,(T) = \text{card}\,(S \cup T) + \text{card}\,(S \cap T) < n.$$

But since we are assuming that $d(a) \geq \frac{n}{2}$ *and* $d(b) \geq \frac{n}{2}$*, we have arrived at a contradiction.* ❑

8.5 Planarity

370 Definition A graph is *planar* if it can be drawn in a plane with no intersecting edges.

371 Example K_4 is planar, as shewn in figure **??**.

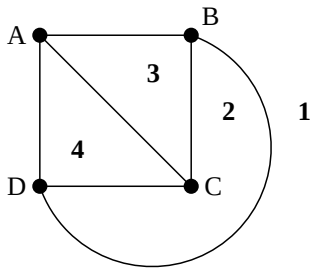

Figure 8.25: Example **??**.

372 Definition A *face* of a planar graph is a region bounded by the edges of the graph.

373 Example From figure **??**, K_4 has 4 faces. Face **1** which extends indefinitely, is called the *outside face*.

374 Theorem (Euler's Formula) For every drawing of a connected planar graph with v vertices, e edges, and f faces the following formula holds:

$$v - e + f = 2.$$

Proof: *The proof is by induction on e. Let* $P(e)$ *be the proposition that* $v - e + f = 2$ *for every drawing of a graph G with e edges. If* $e = 0$ *and it is connected, then we must have* $v = 1$ *and hence* $f = 1$*, since there is only the outside face. Therefore,* $v - e + f = 1 - 0 + 1 = 2$*, establishing* $P(0)$*.*

Assume now $P(e)$ *is true, and consider a connected graph G with* $e+1$ *edges. Either*

1. *G has no cycles. Then there is only the outside face, and so* $f = 1$*. Since there are* $e+1$ *edges and G is connected, we must have* $v = e+2$*. This gives* $(e+2) - (e+1) + 1 = 2 - 1 + 1 = 2$*, establishing* $P(e+1)$*.*
2. *or G has at least one cycle. Consider a spanning tree of G and an edge uv in the cycle, but not in the tree. Such an edge is guaranteed by the fact that a tree has no cycles. Deleting uv merges the two faces on either side of the edge and leaves a graph* G' *with only e edges, v vertices, and* f *faces.* G' *is connected since there is a path between every pair of vertices within the spanning tree. So* $v - e + f = 2$ *by the induction assumption* $P(e)$*. But then*

$$v - e + f = 2 \implies (v) - (e+1) + (f+1) = 2 \implies v - e + f = 2,$$

establishing $P(e+1)$*.*

This finishes the proof. ❑

375 Theorem Every simple planar graph with $v \geq 3$ vertices has at $e \leq 3v-6$ edges. Every simple planar graph with $v \geq 3$ vertices and which does not have a C_3 has $e \leq 2v-4$ edges.

Proof: *If $v = 3$, both statements are plainly true so assume that G is a maximal planar graph with $v \geq 4$. We may also assume that G is connected, otherwise, we may add an edge to G. Since G is simple, every face has at least 3 edges in its boundary. If there are f faces, let F_k denote the number of edges on the k-th face, for $1 \leq k \leq f$. We then have*

$$F_1 + F_2 \cdots + F_f \geq 3f.$$

Also, every edge lies in the boundary of at most two faces. Hence if E_j denotes the number of faces that the j-th edge has, then

$$2e \geq E_1 + E_2 + \cdots + E_e.$$

Since $E_1 + E_2 + \cdots + E_e = F_1 + F_2 \cdots + F_f$, we deduce that $2e \geq 3f$. By Euler's Formula we then have $e \leq 3v-6$.

The second statement follows for $v = 4$ by inspecting all graphs G with $v = 4$. Assume then that $v \geq 5$ and that G has no cycle of length 3. Then each face has at least four edges on its boundary. This gives $2e \geq 4f$ and by Euler's Formula, $e \leq 2v-4$. ❑

376 Example K_5 is not planar by Theorem **??** since K_5 has $\binom{5}{2} = 10$ edges and $10 > 9 = 3(5)-6$.

377 Example $K_{3,3}$ is not planar by Theorem **??** since $K_{3,3}$ has $3 \cdot 3 = 9$ edges and $9 > 8 = 2(6)-4$.

378 Definition A *polyhedron* is a convex, three-dimensional region bounded by a finite number of polygonal faces.

379 Definition A *Platonic solid* is a polyhedron having congruent regular polygon as faces and having the same number of edges meeting at each corner.

By puncturing a face of a polyhedron and spreading its surface into the plane, we obtain a planar graph.

380 Example (Platonic Solid Problem) How many Platonic solids are there? If m is the number of faces that meet at each corner of a polyhedron, and n is the number of sides on each face, then, in the corresponding planar graph, there are m edges incident to each of the v vertices. As each edge is incident to two vertices, we have $mv = 2e$, and if each face is bounded by n edges, we also have $nf = 2e$. It follows from Euler's Formula that

$$\frac{2e}{m} - e + \frac{2e}{n} = 2 \implies \frac{1}{m} + \frac{1}{n} = \frac{1}{e} + \frac{1}{2}.$$

We must have $n \geq 3$ and $m \geq 3$ for a nondegenerate polygon. Moreover, if either n or m were ≥ 6 then

$$\leq \frac{1}{3} + \frac{1}{6} = \frac{1}{2} < \frac{1}{e} + \frac{1}{2}.$$

Thus we only need to check the finitely many cases with $3 \leq n, m \leq 5$. The table below gives the existing polyhedra.

n	m	v	e	f	polyhedron
3	3	4	6	4	tetrahedron
4	3	8	12	6	cube
3	4	6	12	8	octahedron
3	5	12	30	20	icosahedron
5	3	20	30	12	dodecahedron

381 Example (Regions in a Circle) Prove that the chords determined by n points on a circle cut the interior into $1 + \binom{n}{2} + \binom{n}{4}$ regions provided no three chords have a common intersection.

Solution: By viewing the points on the circle and the intersection of two chords as vertices, we obtain a plane graph. Each intersection of the chords is determined by four points on the circle, and hence our graph has $v = \binom{n}{4} + n$ vertices. Since each vertex inside the circle has degree 4 and each vertex on the circumference of the circle has degree $n+1$, the Handshake Lemma (Theorem **??**) we have a total of

$$e = \frac{1}{2}\left(4\binom{n}{4} + n(n+1)\right)$$

edges. Discounting the outside face, our graph has

$$f - 1 = 1 + e - v = 1 + 2\binom{n}{4} + \frac{n^2}{2} + \frac{n}{2} - \left(\binom{n}{4} + n\right) = 1 + \binom{n}{2} + \binom{n}{4}$$

faces or regions.

Homework

382 Problem Determine whether there is a simple graph with eight vertices having degree sequence $6,5,4,3,2,2,2,2$.

383 Problem Determine whether the sequence $7,6,5,4,4,3,2,1$ is graphic.

384 Problem (IMO 1964) Seventeen people correspond by mail with one another—each one with all the rest. In their letters only three different topics are discussed. Each pair of correspondents deals with only one of these topics. Prove that there at least three people who write to each other about the same topic.

385 Problem If a given convex polyhedron has six vertices and twelve edges, prove that every face is a triangle.

386 Problem Prove, using induction, that the sequence

$$n, n, n-1, n-1, \ldots, 4, 4, 3, 3, 2, 2, 1, 1$$

is always graphic.

387 Problem Seven friends go on holidays. They decide that each will send a postcard to three of the others. Is it possible that every student receives postcards from precisely the three to whom he sent postcards? Prove your answer!

Answers

383 Using the Havel-Hakimi Theorem, we have

$$7,6,5,4,4,3,2,1 \to$$
$$5,4,3,3,2,1,0 \to$$
$$3,2,2,1,0,0 \to$$
$$1,1,0,0 \to$$

This last sequence is graphic. Hence the original sequence is graphic.

384 Choose a particular person of the group, say Charlie. He corresponds with sixteen others. By the Pigeonhole Principle, Charlie must write to at least six of the people of one topic, say topic I. If any pair of these six people corresponds on topic I, then Charlie and this pair do the trick, and we are done. Otherwise, these six correspond amongst themselves only on topics II or III. Choose a particular person from this group of six, say Eric. By the Pigeonhole Principle, there must be three of the five remaining that correspond with Eric in one of the topics, say topic II. If amongst these three there is a pair that corresponds with each other on topic II, then Eric and this pair correspond on topic II, and we are done. Otherwise, these three people only correspond with one another on topic III, and we are done again.

385 Let x be the average number of edges per face. Then we must have $xf = 2e$. Hence $x = \dfrac{2e}{f} = \dfrac{24}{8} = 3$. Since no face can have fewer than three edges, every face must have exactly three edges.

386 The sequence $1,1$ is clearly graphic. Assume that the sequence

$$n-1,n-1,\ldots,4,4,3,3,2,2,1,1$$

is graphic and add two vertices, u,v. Join v to one vertex of degree $n-1$, one of degree of $n-2$,, etc., one vertex of degree 1. Since v is joined to $n-1$ vertices, and u so far is not joined to any vertex, we have a sequence

$$n,n-1,n-1,n-1,n-2,n-2,\ldots,4,4,3,3,2,2,1,0.$$

Finally, join u to v to obtain the sequence

$$n,n,n-1,n-1,\ldots,4,4,3,3,2,2,1,1.$$

387 The sequence $3,3,3,3,3,3,3$ is not graphic, as the number of vertices of odd degree is odd. Thus the given condition is not realisable.