Solutions to Exercises
Chapter 2: On numbers and counting

1 Criticise the following proof that 1 is the largest natural number.

> *Let n be the largest natural number, and suppose than $n \neq 1$. Then $n > 1$, and so $n^2 > n$; thus n is not the largest natural number.*

Of course, the flaw is the assumption that there is a largest natural number. The argument shows that, if a largest natural number exists, then it must be equal to 1. But, since 1 is not the largest natural number, it follows that no largest natural number can exist.

Now, on page 36 (or page 188), you will find a proof that a finite ordered set has a largest element. So this is a rather roundabout proof that there are infinitely many natural numbers!

2 Prove by induction that the Odometer Principle with base b does indeed give the representation $x_{n-1}\ldots x_1x_0$ for the natural number

$$N = x_{n-1}b^{n-1} + \cdots + x_1b + x_0.$$

The induction begins because the *digit* 1 does represent the *number* 1.

Now suppose that the digit string $x_{n-1}\ldots x_1x_0$ does represent the number $N = x_{n-1}b^{n-1} + \cdots + x_1b + x_0$. Let m be the largest number such that $x_i = b-1$ for all $i \leq m-1$.

If $m \neq n$, then $x_m \neq b-1$, and so the next string produced by the odometer is $x_{n-1}\ldots y_m00\ldots0$, where y_m is the digit following x_m in sequence (that is, $y_m = x_m + 1$). And

$$\begin{aligned} N+1 &= x_{n-1}b^{n-1} + \cdots + x_mb^m + (b-1)(b^{m-1} + \cdots + 1) + 1 \\ &= x_{n-1}b^{n-1} + \cdots + (x_m+1)b^m, \end{aligned}$$

which is the number represented by the new string. (We used the fact that the sum of the geometric progression $b^{m-1} + \cdots + b + 1$ is equal to $(b^m - 1)/(b-1)$.)

Similarly, if $m = n$, then the old odometer string consists of the digit $b-1$ repeated n times, and the new string is 1 followed by n 0s. We have

$$N+1 = (b-1)(b^{n-1} + \cdots + 1) = b^n,$$

as required.

So the induction step goes through in either case.

3 (a) Prove by induction that

$$n! > \left(\frac{n}{e}\right)^n$$

for $n \geq 1$. (You may use the fact that $(1+\frac{1}{n})^n < e$ for all n.)

(b) Use the arithmetic–geometric mean inequality to show that $n! < \left(\frac{n+1}{2}\right)^n$ for $n > 1$, and deduce that

$$n! < e\left(\frac{n}{2}\right)^n$$

for $n \geq 1$.

(a) Clearly $1! = 1 > 1/e$. Suppose that $n! > (n/e)^n$. Then

$$\begin{aligned} (n+1)! &> (n+1)\left(\frac{n}{e}\right)^n \\ &= \left(\frac{n+1}{e}\right)^{n+1} \cdot \left(\frac{e}{(1+1/n)^n}\right) \\ &> \left(\frac{n+1}{e}\right)^{n+1}, \end{aligned}$$

where in the last line we used the given fact. So the induction goes through.

The fact can be proved using the Binomial Theorem (page 25) and the Taylor series for e^x (page 54) as follows:

$$\begin{aligned} \left(1+\frac{1}{n}\right)^n &= 1 + \frac{1}{1!} + \frac{1}{2!}\left(1-\frac{1}{n}\right) + \frac{1}{3!}\left(1-\frac{1}{n}\right)\left(1-\frac{2}{n}\right) + \cdots \\ &< 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots \\ &= e. \end{aligned}$$

(b) The geometric mean of the numbers $1, 2, \ldots, n$ is the n^{th} root of their product, that is, $(n!)^{1/n}$; their arithmetic mean is their sum divided by n, which is $\frac{1}{2}n(n+1)/n = (n+1)/2$. So the AM-GM inequality gives us that $n! < ((n+1)/2)^n$.

Since $(n+1)^n = n^n(1+\frac{1}{n})^n < en^n$, the final result follows.

The proof of the AM-GM inequality goes as follows. Let $x_1, \ldots, x_n$ be positive numbers. Suppose first that $x_1 = \ldots = x_{n-1} = a$, while $x_n = x$. Then the arithmetic and geometric means are equal to $((n-1)a+x)/n$ and $(a^{n-1}x)^{1/n}$ respectively; so we have to prove that $f(x) = (((n-1)a+x)/n)^n - a^{n-1}x \geq 0$. This clearly holds when $x = a$. Also, we have $f'(x) = (((n-1)a+x)/n)^{n-1} - a^{n-1}$, which is negative for $x < a$ and positive for $x > a$. (If $x < a$, then $(n-1)a + x < na$, and similarly if $x > a$.) So $f(x)$ has a minimum when $x = a$, and thus $f(x) \geq 0$ for all $x > 0$.

Now let r of the x_i be equal, say $x_1 = \ldots = x_r \neq x_{r+1}$. By replacing the elements $x_1, \ldots, x_{r+1}$ by their arithmetic mean repeated $r+1$ times, we don't change the arithmetic mean of the n numbers, but we increase the geometric mean (by the argument in the preceding paragraph). Continue in this way until all the n numbers are equal. Then their AM and GM are equal. But the AM has not been changed, while the GM has been increased. So the AM of the original set must have been at least as big as the GM.

4 (a) Prove that $\log x$ grows more slowly than x^c for any positive number c.
(b) Prove that, for any $c, d > 1$, we have $c^x > x^d$ for all sufficiently large x.

(b) We modify the argument on page 12. We may assume that d is a positive integer (otherwise, just round it up to the next integer). Now

$$c^x = \mathrm{e}^{x \log c} \geq \frac{(x \log c)^{d+1}}{(d+1)!} \geq x^d$$

as long as $x \geq (d+1)!/(\log c)^{d+1}$.

(a) Putting $y = x^c$, we have to show that $\log y^{1/c}$ grows more slowly that y, that is, that $y^{1/c}$ grows more slowly than e^y. This is a special case of (b).

5 (a) We saw that there are $2^{2^3} = 256$ labelled families of subsets of a 3-set. How many unlabelled families are there?
(b) Prove that the number $F(n)$ of unlabelled families of subsets of an n-set satisfies $\log_2 F(n) = 2^n + O(n \log n)$.

(a) Let $\{1,2,3\}$ be the 3-set. A family may include the empty set, or not; and it may include $\{1,2,3\}$, or not. So we count the number of families made up of 1-sets and 2-sets only, and multiply by 4.

If there are no 1-sets, or all possible 1-sets, then the points $1,2,3$ are all alike as far as 1-sets go, and so the 4 possible shapes for the 2-sets (shown on page 15) determine everything. On the other hand, if there are one or two 1-sets, then one point is different from the other two, so instead of four there are six possible shapes for the 2-sets. (With one 2-set, it may contain the special point or not; with two, the special point may lie in both or in just one). So there are $4+4+6+6 = 20$ configurations for the 1-sets and 2-sets, and 80 families of sets altogether.

(b) We have $2^{2^n}/n^n \leq 2^{2^n}/n! \leq F(n) \leq 2^{2^n}$ (see page 15). So $2^n - n \log_2 n \leq \log_2 F(n) \leq 2^n$, from which the result follows.

6 Verify that the numbers of graphs are given in Table 2.1 for $n \leq 5$.

n	2	3	4	5
labelled	2	8	64	1024
unlabelled	2	4	11	34

Table 2.1. Graphs

For labelled graphs on $2,3,4,5$ vertices, there are $1,3,6,10$ pairs of vertices, and for each pair we have to decide whether to join or not; these choices specify the graph completely. So there are $2^1 = 2$, $2^3 = 8$, $2^6 = 64$, $2^{10} = 1024$ labelled graphs in the four cases.

For unlabelled graphs, try to write down all the possibilities: see page 15 for the case $n = 3$. In Chapter 15, you will see a less error-prone method; the value for $n = 4$ is computed on page 253. Drawings of the graphs on at most four vertices appear in N. J. A. Sloane and S. Plouffe, *The Encyclopedia of Integer Sequences*, Academic Press, 1995, Figure M1253, available online here.

7 Suppose that an urn contains four balls with different colours. In how many ways can three balls be chosen? As in the text, we may be interested in the order of choice, or not; and we may return balls to the urn, allowing repetitions, or not. Verify the results of Table 2.2.

	order important	order unimportant
repetition allowed	64	20
repetition not allowed	24	4

Table 2.2. Selections

Consider first the case where order is important. If repetitions are allowed, then each of the three balls chosen can have any of the four colours, giving $4 \cdot 4 \cdot 4 = 64$ possibilities. If repetitions are not allowed, there are still 4 possibilities for the first ball, but only 3 for the second and 2 for the third, total $4 \cdot 3 \cdot 3 = 24$.

If order is not important, all three balls could be the same colour (four possibilities); or two of one colour and one of another ($4 \cdot 3 = 12$ possibilities, since there are four choices for the repeated colour and then three for the other colour); or all different (four possibilities, since the one missing colour determines the other three). Thus there are 20 selections, of which 4 have no repetitions.

8 A *Boolean function* takes n arguments, each of which can have the value TRUE or FALSE. The function takes the value TRUE or FALSE for each choice of values of its arguments. Prove that there are 2^{2^n} different Boolean functions. Why is this the same as the number of families of sets?

Let $x_1, \ldots, x_n$ be the n arguments. There are two choices for the value of each, and hence 2^n for the number of different "inputs". For each input the function takes one of two possible values. The values on the different inputs specify the function. So there are $2^{(2^n)}$ different functions.

Let $X = \{1, 2, \ldots, n\}$. An input to the function can be regarded as the characteristic function of a subset Y of X (the set of values i for which x_i takes the value TRUE). Now we have specified the function if we know which sets correspond to inputs giving the function the value TRUE. Thus a family of sets specifies a function, and *vice versa*.

9 Logicians define a natural number to be the set of all its predecessors: so 3 is the set $\{0, 1, 2\}$. Why do they have to start counting at 0?

Suppose that we start counting at 1 instead of 0. Either we define 3 to be the set of *strict* predecessors of 3, in which case there are only two of them (1 and 2); or we allow non-strict predecessors, in which case 3 is a member of itself, which leaves us vulnerable to *Russell's paradox* about the set of sets which are not members of themselves (see page 308).

10 A function f has *polynomial growth* of degree d if there exist positive real numbers a and b such that $an^d < f(n) < bn^d$ for all sufficiently large n. Suppose that f has polynomial growth, and g has exponential growth with exponential constant greater than 1 (as defined in the text). Prove that $f(n) < g(n)$ for all sufficiently large n. If $f(n) = 10^6 n^{10^6}$ and $g(n) = (1.000001)^n$, how large is 'sufficiently large'?

The first part is similar to Question 4.

For the second part, $n = 10^{14}$ suffices. For we have

$$g(10^{14}) = (1.000001)^{10^{14}} \geq 1 + 10^{14} \cdot (0.000001) > 10^8,$$

the first inequality by the Binomial Theorem; whereas

$$f(10^{14}) = 10^6 \cdot 10^{14 \times 10^6} = 10^{0.14000006 \times 10^8}.$$

11 Let $\mathcal{B}$ be a set of subsets of the set $\{1,2,\dots,v\}$, containing exactly b sets. Suppose that

- every set in $\mathcal{B}$ contains exactly k elements;
- for $i = 1,2,\dots,v$, the element i is contained in exactly r members of $\mathcal{B}$.

Prove that $bk = vr$.

Give an example of such a system, with $v = 6$, $k = 3$, $b = 4$, $r = 2$.

This exercise uses the double counting principle. So let $\mathcal{B} = \{B_1,\dots,B_b\}$, and let $A = \{1,\dots,v\}$ and $B = \{1,\dots,b\}$; let S be the set of pairs (i,j) for which $i \in B_j$. Then every member of A is in r pairs in S, whereas every member of B is in k such pairs. So $bk = vr$ by (2.6.2).

An example is $\mathcal{B} = \{123,145,246,356\}$, where 123 is short for $\{1,2,3\}$, and so on.

12 The ‘Russian peasant algorithm’ for multiplying two natural numbers m and n works as follows.

(2.7.3) Russian peasant multiplication
to multiply two natural numbers m and n

- Write m and n at the head of two columns.
- REPEAT the sequence
  - halve the last number in the first column (discarding the remainder) and write it under this number;
  - double the last number in the second column and write it under this number;

  UNTIL the last number in the first column is 1.

For each even number in the first column, delete the adjacent entry in the second column. Now add the remaining numbers in the second column. Their sum is the answer.

Problems

(i) Prove that this method gives the right answer.

(ii) What is the connection with the primary school method of long multiplication?

(iii) Suppose we change the algorithm by squaring (instead of doubling) the numbers in the second column, and, in the last step, multiplying (rather than adding) the undeleted numbers. Prove that the number calculated is n^m. How many multiplications does this method require?

(i) Write m to base 2: $m = a_0 + a_1 2 + a_2 2^2 + \ldots + a_r 2^r$, where each a_i is zero or one. Counting the first row as number 0, the i^{th} number in the first column is $a_i + a_{i+1}2 + \ldots + a_r 2^{r-i}$, and in the second column $2^i \cdot n$. So the rows which remain after the deletions are those for which $a_i = 1$, and the final total is

$$\sum_{a_i=1} 2^i \cdot n = \sum_{i=0}^{r} a_i 2^i \cdot n = m \cdot n,$$

as required.

(ii) Suppose that we do the long multiplication $n \times m$ in base 2. (Note the changed order!) Now m is given by the digit sequence $a_r \dots a_1 a_0$. If $a_i = 0$, we ignore it; if $a_i = 1$, we shift m left i places (which has the effect of multiplying it by 2^i), multiply it by 1 (which doesn't change it), and write it down. Now we add up all these numbers, which clearly gives exactly the same sum as before.

(iii) With these changes, the number in the i^{th} row and second column is n^{2^i}, and the final answer is

$$\prod_{a_i=1} n^{2^i} = \prod_{i=0}^{r} n^{a_i 2^i} = n^m.$$

We have used only $2r$ multiplications, where $r = \lceil \log_2 m \rceil$, as opposed to the $m-1$ multiplications required by the simple-minded method.

13 According to the Buddha,

> *Scholars speak in sixteen ways of the state of the soul after death. They say that it has form or is formless; has and has not form, or neither has nor has not form; it is finite or infinite; or both or neither; it has one mode of consciousness or several; has limited consciousness or infinite; is happy or miserable; or both or neither.*

How many different possible descriptions of the state of the soul after death do you recognise here?

One could argue here that the numbers of choices should be multiplied, not added; there are 4 choices for form, 4 for finiteness, 2 for modes of consciousness, 2 for finiteness of consciousness, and 4 for happiness, total $2^8 = 256$. (You may wish to consider whether all 256 are really possible.)

14 The library of Babel (Jorge Luis Borges, *Labyrinths*, 1964) consists of interconnecting hexagonal rooms. Each room contains twenty shelves, with thirty-five books of uniform format on each shelf. A book has four hundred and ten pages, with forty lines to a page, and eighty characters on a line, taken from an alphabet of twenty-five orthographical symbols (twenty-two letters, comma, period and space). Assuming that one copy of every possible book is kept in the library, how many rooms are there?

Each book is made up of $410 \cdot 40 \cdot 80 = 1312000$ characters chosen from a set of 25, so there are $25^{1312000}$ different books. Each room of the library contains $20 \cdot 35 = 700$ books. So there are $25^{1312000}/700$ rooms. This number is approximately

$2.794 \times 10^{1834094}$. (By comparison, the number of elementary particles in the universe is thought to be around 10^{80}.)

The text of Borges' story and a picture of the Library of Babel are available here. Further discussion can be found here.