As you can see, induction can be a very powerful tool for proving statements about positive integer n, especially formulas involving n. But often these formulas have to be "guessed" by finding patterns, so induction goes hand-in-hand with "guess and check."

10/17 <u>Strong form of Mathematical Induction</u> § 2.5

Sometimes when proving things by induction it can be helpful to know that $P(k)$ is true for <u>all</u> $k < n$ to show $P(n)$ is true (and not just $P(n-1)$). The <u>Strong Principle of Induction</u> says that if:

- $P(n_0)$ is true for some n_0 (base case)
- $P(n)$ is true whenever $P(k)$ is true for all $n_0 \leq k < n$, for all $n \geq n_0$,

then $P(n)$ is true for all $n \geq n_0$.
(Notice also how we allow n_0 to be different from 1).

<u>E.g.</u> <u>Thm</u> Using 2¢ and 5¢ stamps, we can make any amount n¢ for all $n \geq 4$.

<u>Pf</u>: We can use <u>two</u> base cases: $n = 4$¢ $= 2$¢ $+ 2$¢ and $n = 5$¢ (one 5 cent stamp). Then for $n \geq 6$: we know by the <u>strong</u> principle of induction that we can make $(n-2)$¢ with those stamps, so just add a 2¢ stamp to make n¢. (Notice we needed $(n-2)$ and not $(n-1)$.) ☒

Here's another example of strong induction:

The Fibonacci numbers F_n for $n \geq 1$ are defined by $F_1 = 1$ and $F_2 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for $n > 2$.

E.g. $F_3 = F_1 + F_2 = 1+1 = 2$
$F_4 = F_2 + F_3 = 1+2 = 3$
$F_5 = F_3 + F_4 = 2+3 = 5$ . . .

Thm $F_n \leq 2^{n-1}$ for all $n \geq 1$.

Pf: We use strong induction. We have two base cases: $n=1 \rightsquigarrow F_1 = 1 \leq 2^0 = 2^{1-1}$ ✓
$n=2 \rightsquigarrow F_2 = 1 \leq 2^1 = 2^{2-1}$ ✓

Now, for $n > 2$, assume that $F_{n-1} \leq 2^{n-2}$ and $F_{n-2} \leq 2^{n-3}$ (using strong induction).

Thus, $F_n = F_{n-2} + F_{n-1}$
$\leq 2^{n-3} + 2^{n-2}$ (by induction)
$\leq 2^{n-2} + 2^{n-2} = 2 \cdot (2^{n-2}) = 2^{n-1}$

and so by induction we are done! ☒

The strong form of induction is closely related to the well-ordering property for the nonnegative integers, which says that every nonempty set of nonnegative numbers has a minimum.

You can see in the book how the W.O.P. can be used to show we always get a well-defined quotient and remainder when doing long division.

10/19

Basic Mathematical Structures: Functions §3.1

Having concluded our study of proofs (Chapter 2), we are starting a new chapter, Chapter 3, which discusses basic mathematical structures. The most basic mathematical structures are sets, which we have already discussed in Chapter 1. The next most basic structures in math are functions, which are procedures for going from one set to another.

There are many ways to think about functions. One is that a function f from a set X to a set Y is a machine or a rule that takes something in X and spits out something in Y:

$$x \in X \Longrightarrow \underbrace{\boxed{\; f \;}}_{\text{machine}} \Longrightarrow y = f(x) \in Y$$

For example, consider the following procedure:

- given a 10-digit number x like
  $x = 1043213598$
  we sum together all the digits:
  $1+0+4+3+2+1+3+5+9+8 = 3\underline{\underline{6}}$

  and then "spit out" the ones digit of the resulting sum as our $y = f(x)$ (here $y = 6$ in the example).

This describes a function f whose domain X is the set of 10-digit numbers and codomain Y is the set of one digit numbers.

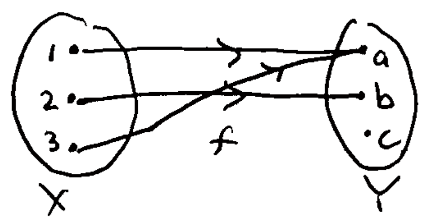
(This is a simplification of the "check sum" procedure for credit card numbers; the book describes the real procedure, which is more complicated.)

[Notice that the domain of function f is the name we give to the input set X and codomain is the name we give to the output set Y.]

That was an intuitive definition of function as machine. The formal definition of function uses ordered pairs.

Def'n A function from set X (called the domain) to set Y (called the codomain) is a subset of $X \times Y$ (set of ordered pairs (x,y) w/ $x \in X$, $y \in Y$), such that: for every $x \in X$, there is a unique $y \in Y$ with (x,y) in our subset.

E.g. We often represent functions by arrow diagrams:



This corresponds to the subset $\{(1,a), (2,b), (3,c)\}$ of $X \times Y$ with $X = \{1,2,3\}$ and $Y = \{a,b,c\}$. Notice how for every $x \in X$ there is a unique $y \in Y$ with (x,y) in our subset: we write $f(x) = y$ for this y. In this case:

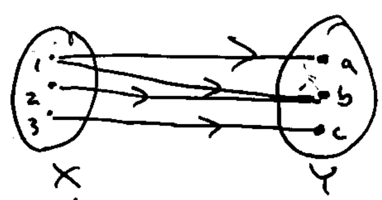
$f(1) = a$
$f(2) = b$
$f(3) = a$

The function is named "f" here.

In our credit card checksum example function we had $f(104321359\,8) = 6$, and more generally the ordered pairs in our subset will always be $\boxed{\{(x, f(x))\}}$ so we use "f" as shorthand for the function.

The set $\{f(x) : x \in X\}$ of values our function f actually takes on is called the range of f, and it is a subset of the codomain:
e.g. in the arrow diagram example f above the codomain was $Y = \{a, b, c\}$, but the range is $\{a, b\}$ since there is no $x \in X$ w/ $f(x) = c$.

We also write $f : X \to Y$ to mean f is a function from X to Y. The arrow helps you remember what it does: it takes something in X to something in Y.
A diagram like:



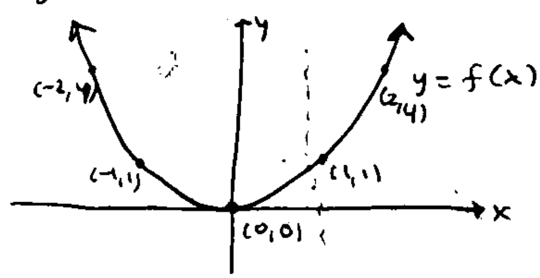
is not the arrow diagram of a function because the key property of a function is that for every $x \in X$ there is a unique $f(x) = y \in Y$ it is "sent to" and here 1 is "sent" to both a and b!

From calculus you are probably used to function like

$$f(x) = x^2$$

whose domain and codomain are the real numbers $\mathbb{R}$. Notice how "$f(x) = x^2$" is the "rule/machine" description of the function: it tells us for a given input x how to produce the output of the function; e.g. $f(3) = 3^2 = 3 \times 3 = 9$.

But we can also represent a function $f : \mathbb{R} \to \mathbb{R}$ by its <u>graph</u> like we are used to doing:

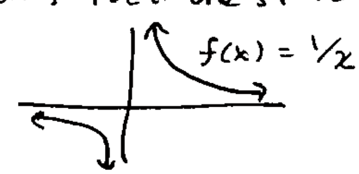


The graph of a function $f : \mathbb{R} \to \mathbb{R}$ is just a drawing of all the points $\{(x, f(x)) : x \in \mathbb{R}\}$, i.e., it is another visual representation of the ordered pair definition of function. (<u>Recall</u>: "Vertical line test")

Some functions defined algebraically like

$$f(x) = 1/x$$

have domains that are strict <u>subsets</u> of $\mathbb{R}$:



Here the domain (and range) of $f(x) = 1/x$ is $\{x \in \mathbb{R} : x \neq 0\}$ since we are not allowed to divide by zero.

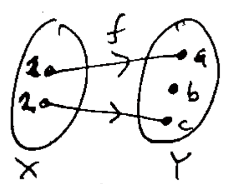
10/26 §3.1

More about functions: Let $f: X \to Y$ be a function.

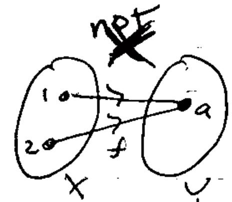
Def'n The function f is called one-to-one (or injective) if there are not two different $x_1, x_2 \in X$ with $f(x_1) = f(x_2)$.

"Everything in X is sent to a different thing in Y"

E.g.



one-to-one



not one-to-one

E.g. Let $f: \mathbb{Z} \to \mathbb{Z}$ (integers) be given by $f(n) = 2n+1$.

(so $f(0)=1$, $f(1)=3$, $f(-1)=-3$...)

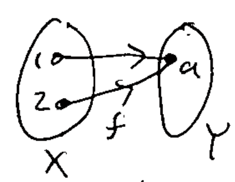
This f is one-to-one since if $2n_1+1 = 2n_2+1$ then $n_1 = n_2$. ✓

Def'n The function f is called onto (or surjective) if for every $y \in Y$, there is some $x \in X$ with $f(x) = y$.

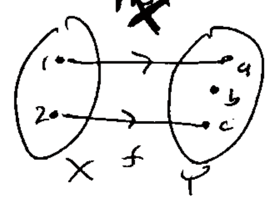
"Everything in Y is mapped to by something in X"

Onto same as: range = codomain.

E.g.



onto

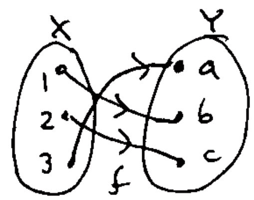


not onto

E.g. If $f: \mathbb{Z} \to \mathbb{Z}$ is given by $f(n) = 2n+1$ then f is not onto since there is no $n \in \mathbb{Z}$ w/ $2n+1 = 0$ (or any even number).

Def'n The function f is called <u>bijective</u> (or a bijection) if it is both one-to-one and onto.

E.g.



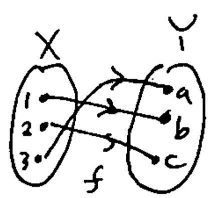
is bijective.

E.g. $f(n) = n+1 : \mathbb{Z} \to \mathbb{Z}$ is a bijection. (<u>why</u>?)

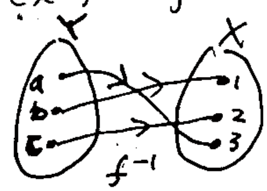
<u>Exercise</u> If $f: X \to Y$ is a bijection between <u>finite</u> sets X and Y, then $\# X = \# Y$ (the sets have same # of elements).

Def'n If $f: X \to Y$ is a bijection, then we define its <u>inverse function</u> $f^{-1}: Y \to X$ by $f^{-1}(y) = x$ if and only if $f(x) = y$.

E.g.

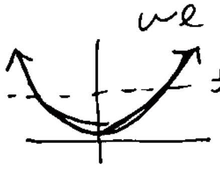


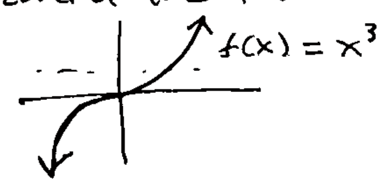
has inverse



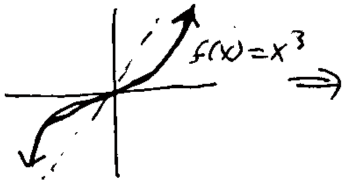
"flip arrows"

E.g. To check that a function $f: \mathbb{R} \to \mathbb{R}$ is one-to-one we have the "horizontal line test"

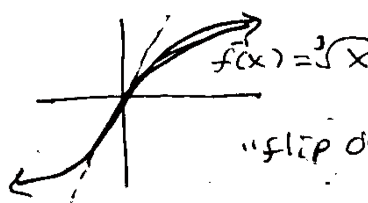




The inverse of $f(x) = x^3$ is $f^{-1}(x) = \sqrt[3]{x}$



$\Rightarrow$



"flip over line $y = x$"

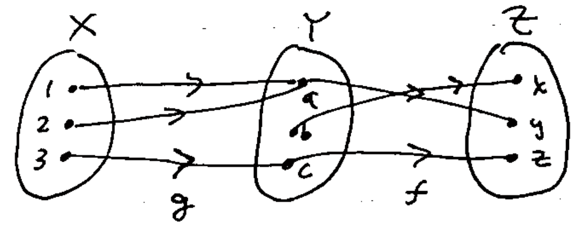
10/24

The inverse function f^{-1} "undoes" whatever f does. Let's make this precise by talking about composition.

Def'n Let $g: X \to Y$ and $f: Y \to Z$ be two functions. Their composition $(f \circ g): X \to Z$ is defined by $(f \circ g)(x) = f(g(x))$ for all $x \in X$.

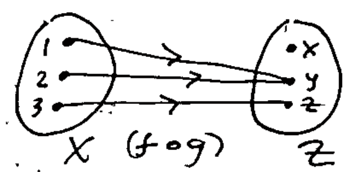
"Do g first and then do f to what you get."

E.g.



"combine arrow diagrams" to form arrow diagram of composition

$\Rightarrow$



E.g. If $f(x) = 2^x : \mathbb{R} \to \mathbb{R}$ and $g(x) = x^3 : \mathbb{R} \to \mathbb{R}$

Then $(f \circ g)(x) = 2^{x^3}$ and $(g \circ f)(x) = (2^x)^3 = 2^{3x}$.

Notice how $(f \circ g) \neq (g \circ f)$! Order matters.

Def'n The identity function $Id_X: X \to X$ on a set X is function with $Id_X(x) = x \quad \forall x \in X$.

"The identity function 'does nothing': gives input as output"

If $f: X \to Y$ is a bijection then

$(f^{-1} \circ f) = Id_X$ identity.

Since $f^{-1}(f(x)) = x \quad \forall x \in X$. This is sense in which inverse function "undoes" original.

Modular arithmetic functions

Many of the functions you're familiar with from calculus, especially linear functions like $f(x) = 5x - 2$ and polynomials like $f(x) = 3x^3 - 2x^2 + 4x - 1$ are important in discrete math too...

The "modulo n" function is another function that's very important in discrete math, and may be new to you.

Def'n Let n be a positive integer. For any integer $m \in \mathbb{Z}$, $m \bmod n$ ("m modulo n") is the unique $r \in \{0, 1, 2, \ldots, n-1\}$ such that r is the remainder when dividing m by n, i.e. $\exists k \in \mathbb{Z}$ such that $m = k \cdot n + r$.

E.g. $3 \bmod 5 = 3$ and $8 \bmod 5 = 3$ too since $8 = 5 + 3$.

$1247 \bmod 10$ is 7 since we just look at 1s place.

For any n, $n \bmod n = 0$, and $-1 \bmod n = n-1$.

In this way, for every positive integer n we get a function $f: \mathbb{Z} \to \mathbb{Z}$ given by $f(m) = m \bmod n$. (The range of f is $\{0, 1, \ldots, n-1\}$ so we could take the codomain to be $\{0, 1, \ldots, n-1\}$ instead...)

The mod n functions can be useful for clock or calendar problems, e.g.:

Exercise If the first day of the year is a Tuesday, what day of the week is the 100th day of the year?

10/26 Sequences §3.2

A sequence is a list of things, like:

1, 2, 3, 4, 5, ...

2, 4, 8, 16, 32, ...

1, 2, 3 etc.

b, a, n, a, n, a

It can be finitely long, or infinitely long.
It can have repetitions (like in the letters of "banana")
The important thing is that the order of a sequence matters, so $1,2,3 \neq 3,1,2$.

Formally, we can represent a sequence by a function s whose domain is a subset of the positive integers. (which we denote by $\mathbb{Z}_{>0}$ or $\mathbb{Z}^+$)

E.g. $s: \mathbb{Z}_{>0} \to \mathbb{Z}$
with $s(n) = n$ gives the sequence $1, 2, 3, 4, \ldots$

E.g. $s: \mathbb{Z}_{>0} \to \mathbb{Z}$
with $s(n) = 2^n$ gives sequence $2, 4, 8, 16, \ldots$

E.g. $s: \{1,2,3,4,5,6\} \to \{a, b, n\}$
with $s(1) = b$, $s(2) = a$, $s(3) = n$, $s(4) = a$, $s(5) = n$, $s(6) = a$
gives the sequence b, a, n, a, n, a

Usually the domain is either all of $\mathbb{Z}_{>0}$ (for an infinite sequence) or $\{1,2,3,4,\ldots,n\}$ (for a finite sequence)

We write the sequence as $s_1, s_2, s_3, \ldots$
where $s_i := s(i)$ is "sequence notation".
We also sometimes write it as $\{s_n\}_{n=1}^{\infty}$.

If the codomain of the sequence s is a set of numbers, we say s is <u>increasing</u> if $s_i < s_j$ when $i<j$ and say s is <u>decreasing</u> if $s_i > s_j$ when $i<j$.

E.g. $2, 4, 8, 16, 32, \ldots$ is increasing and $\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}, \ldots$ is decreasing.

We define <u>nonincreasing</u> sequences (w/ $s_i \geq s_j$) and <u>nondecreasing</u> seq. (w/ $s_i \leq s_j$) similarly.

If we have a finite sequence $\{s_n\}_{n=1}^{k}$, we define its <u>sum</u> $\sum_{n=1}^{k} s_n = s_1 + s_2 + \cdots + s_k$.

E.g. We already saw (using induction) that

$$2^0+2^1+2^2+\cdots+2^k = \sum_{n=1}^{k+1} 2^{n-1} = 2^{k+1}-1.$$

Can define <u>product</u> $\prod_{n=1}^{k} s_n = s_1 \times s_2 \times \cdots \times s_k$ as well.

If s is a sequence, a <u>subsequence</u> of s is a sequence we get by selecting some of the items of the list s (not necessarily consecutive) in the <u>same order</u>!

E.g. <u>b, a</u> is a subsequence of <u>b, a, n, a, n, a</u>, as is <u>b, n</u> and <u>a, a, a</u> and <u>n, n</u>, but <u>a, b</u> is <u>not</u> a subsequence of <u>b, a, n, a, n, a</u>.

If the sequence is $\{s_n\}$ then the subsequence will be $s_{n_1}, s_{n_2}, s_{n_3}, \ldots$ where $\{n_1 < n_2 < \cdots\}$ is a subset of the domain of s.

E.g. $2, 4, 6, 8, \ldots$ is a subsequence of $1, 2, 3, 4, 5, \ldots$

Strings §3.2 If X is a finite set, then a string over X is any finite sequence of elements from X. We use X^* to denote all strings over X.

E.g. If $X = \{a, b\}$ then some elements of X^* are
a, b, aa, ab, bba, $baba$, etc.

Another string that's always in X^* is the null string, denoted λ, that doesn't have any letters.

If $\alpha, \beta \in X^*$ are two strings, their concatenation $\alpha\beta$ is what we get by putting α right before β:

E.g. $\alpha = aba$, $\beta = bba$, then $\alpha\beta = ababba$.

Notice that the length (# of letters in) $\alpha\beta$ is the sum of length of α and length of β.

Finally, a substring of $\alpha \in X^*$ is a string of consecutive letters from α.

E.g. $\alpha = aba$ then ab and ba are substrings, but ba is not.

Exercise Show β is a substring of α if and only if $\alpha = \delta\beta\gamma$ for some strings δ and γ. //