

### Stuff about Proofs and Other Phenomena (S-POP)

#### Part A: Generalities on understanding and explaining mathematics

Look, math is hard. Let's just get that out of the way. But there are things you can do to make it easier. One of the central themes behind this course is that:

You can make math easier, for your audience and, especially, for **yourself**, by making the effort to *communicate* mathematics properly.

The key is the word “properly.” What does that mean? We'll spend considerable time, in this course, exploring and addressing this issue. And at the end of the semester, *you* can tell *me*, and *your classmates*, what (you think) it means.

In the meantime, here are some general tips. First of all: be *clear*. Clarity in mathematical (as in any other form of) expression is a common courtesy. Your intended audience will thank you if you avoid sloppiness and rambling; if you think out what you are going to say before you say it, and so on.

In this class, your classmates and I are your intended audience. Show us the courtesy of clarity, and we'll be kind to you in return. (Certainly *I* will be kind to you in return. Perhaps I shouldn't speak for your classmates, but I'm assuming they know what's good for them, so....)

At least as important is this fact: clarity of presentation not only **reflects**, but it also **reinforces**, clarity of thought. That is: making the effort to communicate clearly will not only help you *impress* with your abilities; it will also help *sharpen* your abilities.

Besides being clear, you should strive, in your mathematical communication, to be *complete*, *concise*, and, of course, *correct*. Perhaps “Communicate clearly, completely, concisely, and correctly” is not a bad mantra, if you're into that sort of thing. But note that the word “correctly” here, though it appears last, should not be taken as the *last word* in mathematics.

This is not to say that correctness is *less* important than the above other three C's of mathematical communication. And we're certainly not suggesting that, in this course, you should aim for the *wrong* answer. It's just that, in this course, you will be asked to be mindful, more than you are perhaps used to, of those other three C's.

What we said above concerning clarity in your mathematical work also applies to completeness, conciseness, and correctness: attending to these will help you wrap your own brain around the ideas as much as it will help others.

To be clear (and complete, concise, and correct): we will spend at least as much time, in this course, *doing* mathematics as we will *communicating* mathematics. This is a math course, not a communications course (per se). The focus on communication, while something of an end in itself, is, at least as significantly, a *means* to the end of becoming better, more fluent, more capable *practitioners* of the art of mathematics. Yes, it is an art. Math is, among other things, a *creative* endeavor.

A painter isn't finished as soon as she can visualize her work in her head, is she? The creative process really takes hold in the translation of the ideas to their expression on canvas. And so it is with mathematics.

#### Part B: “Shoulds” and “shouldn'ts” of mathematical communication

The above observations are quite general, which is a good thing, 'cause otherwise calling them “generalities” would be misleading.

We'll certainly want to examine some *particulars* of mathematical communication, as well. OK, let's. We start with the following very brief list.

- When communicating mathematics, one *should*: **speak in complete sentences.**

The nice thing about math (well, one nice thing, anyway; there are many others) is that complete sentences can be quite brief: for example, “ $x = 2$ ” is a complete sentence. Ya got yer subject, ya got yer verb, ya got yer object; hey, what else do ya need?

- When communicating mathematics, one *shouldn't*: **use symbols like “ $\Rightarrow$ ” or “ $\rightarrow$ ” to mean “equals.”**

The symbol “ $\Rightarrow$ ” means “implies” (example:  $S$  is a square  $\Rightarrow S$  has four right angles; see Section C(i) below); the symbol “ $\rightarrow$ ” means “converges to” or “approaches” (example:  $\lim_{x \rightarrow 0} (\sin x)/x = 1$ ; see Section C(iv) below). Please do not use either of these symbols to denote equality.

NOW DIG THIS: at least twice over the course of this semester, you will be asked to submit your *own* list of (half a dozen or so) mathematical “shoulds” and “shouldn'ts.” Each item on your list should begin like one of the above two: that is, either with

“When communicating mathematics, one *should*.”

or with

“When communicating mathematics, one *shouldn't*.”

Moreover, each of your “shoulds” and “shouldn'ts” should include a brief explanation/discussion, like those given above.

See Section 5.3 (pages 107–109) of T-BOP (The Book of Proof) for more mathematical “shoulds” and “shouldn'ts.” We'll discuss the “shoulds/shouldn'ts” course requirement further as we proceed.

### Part C: Some varieties of mathematical proof

What follows is a brief, and by no means exhaustive (though perhaps a bit tiring), introduction to various varieties and strategies of mathematical argument and proof. (Most of this is also covered in T-BOP.)

#### Section C(i): $P \Rightarrow Q$ and related results.

If  $P$  and  $Q$  are statements of any kind, then the statement “ $P \Rightarrow Q$ ,” read “ $P$  implies  $Q$ ,” means anytime  $P$  is true,  $Q$  follows. Other ways of saying “ $P \Rightarrow Q$ ” are: “if  $P$ , then  $Q$ ,” “ $Q$  if  $P$ ,” “ $P$  only if  $Q$ .”

To be more precise about what “ $P \Rightarrow Q$ ” means, from a formal point of view, we'd need to get into truth tables and so on. We'll do this later (maybe). For now, we take it on faith that we understand a statement like “today is Saturday implies it's the weekend.” (Convince yourself that

this statement has the same meaning as “if today is Saturday, then it’s the weekend,” “it’s the weekend if today is Saturday,” “today is Saturday only if it’s the weekend.”)

The so-called *direct proof* of a statement like  $P \Rightarrow Q$  goes as follows (we will discuss other methods of proof a bit later):

**Proposition C(i)-1.**  $P \Rightarrow Q$ .

*Proof.* Assume  $P$ . [Anything you see in square-brackets is intended not as part of the proof in question, but as a note about what’s going on. In this case, what’s going on is that you have to do some stuff here to get to the point where you can conclude:] Therefore,  $Q$ .

So  $P \Rightarrow Q$ . **ATWMR**

*Remark.* You should always end a proof with some kind of clear indication that you are done. Here we have used “ATWMR,” which stands for “And There Was Much Rejoicing,” a particularly happy way to end a proof. (And thanks to Monty Python.) If you prefer, use “QED” or a box (“ $\square$ ”) or something, but DO mark the completion of each proof in some definite way. (Come up with your own way; be creative!)

To illustrate Proposition C(i)-1, let’s recall that an *even number* is an integer that equals  $2k$  for some integer  $k$ ; an *odd number* is an integer that equals  $2k - 1$  for some integer  $k$ . We have:

**Proposition C(i)-1<sub>E</sub>.** If  $n$  is an even number then  $n - 1$  is an odd number.

*Proof.* Assume  $n$  is an even number. We may write  $n = 2k$  for some  $k \in \mathbb{Z}$ . But then  $n - 1 = 2k - 1$ , so  $n - 1$  is odd.

So if  $n$  is an even number, then  $n - 1$  is an odd number. **ATWMR**

(The “E” in the subscript of Proposition C(i)-1<sub>E</sub> indicates that this proposition *exemplifies* Proposition C(i)-1.)

**Exercise C(i)-1.** (a) Prove that the sum of two odd numbers is even. (b) Prove that the product of two odd numbers is odd.

**Exercise C(i)-2.** (a) Prove that, if  $n$  is an even number, then  $n^2$  is divisible by 4. (b) Prove that, if  $n$  is an odd number, then  $n^2 - 1$  is divisible by 4.

**Exercise C(i)-3.** Let  $a$ ,  $b$ , and  $c$  be integers. (a) Prove that, if  $a|b$  and  $a|c$ , then  $a|(b + c)$ . (b) Prove that, if  $a|b$ , then  $a|nb$  for any integer  $n$ .

We next note that the statement  $P \Rightarrow Q$  is (always, always, ALWAYS) logically equivalent to its *contrapositive*: the latter is, by definition, the statement  $\sim Q \Rightarrow \sim P$ . Here, the symbol “ $\sim$ ” stands for “not:” so  $\sim P$  means “not  $P$ ,” or “the negation of  $P$ .” (Sometimes you’ll see “ $\neg$ ” used in place of “ $\sim$ .”) Think about it: for example, the contrapositive of “if today is Saturday, then it’s the weekend” is “if it’s not the weekend, then today is not Saturday.” The two statements mean the same thing.

We can therefore also prove  $P \Rightarrow Q$  by *contraposition*, as follows:

**Proposition C(i)-2.**  $P \Rightarrow Q$ .

*Proof.* Assume  $\sim Q$ . [Do what you got to, to get to:] Therefore,  $\sim P$ .

So  $P \Rightarrow Q$ . **ATWMR**

For example:

**Proposition C(i)-2<sub>E</sub>.** If  $m^2$  is an odd number, then  $m$  is an odd number.

*Proof.* Suppose  $m$  is not odd. Then  $m$  is even, so  $m = 2k$  for some  $k$ . But then  $m^2 = (2k)^2 = 4k^2 = 2(2k^2)$ , so  $m^2$  is even, and hence not odd.

So if  $m^2$  is odd, then  $m$  is odd. **ATWMR**

*Remark.* In the above proof, we used the fact that every integer  $m$  must be either even or odd (but not both). This may seem obvious, but is worth explaining. It follows from the *division algorithm*, which tells us we can perform integer division of 2 into  $m$ , to get a unique integer quotient  $k$  and a unique non-negative integer remainder  $r$ , and this remainder must be less than the divisor 2. That is,  $m = 2k + r$  where  $k$  and  $r$  are integers, and either  $r$  equals 0 (in which case  $m$  is even) or 1 (in which case  $m$  is odd).

More generally, the division algorithm tells us that, given a positive integer  $b$  and an integer  $m$ , we can divide  $b$  into  $m$  to get unique integer quotient  $q$  and remainder  $r$ , where  $r$  is non-negative but less than the divisor. That is, given such  $m$  and  $b$ , there are unique integers  $q$  and  $r$  with  $m = bq + r$  and  $0 \leq r < b$ . The division algorithm also probably seems pretty obvious, or at least familiar. But in fact, it follows from a fairly deep fact, called the *well-ordering principle*, concerning the integers. See T-BOP, pages 29-30. We won't discuss this further, except to say that what's obvious in mathematics is sometimes quite profound. (In fact, often, the more obvious, the more profound.)

**Exercise C(i)-4.** Supply a proof by contraposition of Proposition C(i)-1<sub>E</sub>.

**Exercise C(i)-5.** Supply a direct proof of Proposition C(i)-2<sub>E</sub>. Hint: Suppose  $m^2$  is odd. Then we can write  $m^2 = 2\ell + 1$  where  $\ell$  is an integer. Now write  $m = 2k + r$ , where  $k$  is an integer, and  $r$  equals either 0 or 1. (Why can we write  $m$  this way?) Now we have two different ways of writing  $m^2$ ; set them equal, do some algebra, and see what you can deduce about  $r$ .

**Exercise C(i)-6.** Using contraposition prove that, if  $n$  is not divisible by 4, then  $n$  is not divisible by 12.

Whether, in a given instance, to use the direct or the contraposition method to prove  $P \Rightarrow Q$  comes down to a matter of choice; which one seems to work better in the given situation?

**WARNING:**  $P \Rightarrow Q$  is *not* logically equivalent to its *converse*, meaning the statement  $Q \Rightarrow P$ . For example, “If today is Saturday then it’s the weekend” is not equivalent to “If it’s the weekend, then today is Saturday.” (After all, if it’s the weekend, it might be Sunday.) So don’t ever try to prove  $P \Rightarrow Q$  by assuming  $Q$ , and deducing  $P$ .

Incidentally, in the above paragraph, we have demonstrated that the statement “If it’s the weekend, then today is Saturday” is false by the method of *counterexample*. That is, we have produced a *single* scenario where the statement doesn’t hold. In general, to prove that a statement  $X \Rightarrow Y$  is false, it’s enough to exhibit a single situation where  $X$  holds but  $Y$  doesn’t.

**Exercise C(i)-7.** Consider the statement:

If  $x$  is odd, then  $x$  is divisible by 3.

Prove that this statement is false, using the method of counterexample.

**Exercise C(i)-8.** Consider the converse to the statement of Exercise C(i)-3(a). Is this converse statement true? If so, prove it. If not, show that it's false by counterexample.

Finally, we note that the statement  $P \Leftrightarrow Q$ , read “ $P$  if and only if  $Q$ ,” or more briefly “ $P$  iff  $Q$ ,” by definition means  $P \Rightarrow Q$  and  $Q \Rightarrow P$ . One way to prove  $P \Leftrightarrow Q$  is to demonstrate one at a time the two statements it comprises – that is:

**Proposition C(i)-3.**  $P \Leftrightarrow Q$ .

*Proof.* (a) First we show that  $P \Rightarrow Q$ : assume  $P$ . [Do some stuff in here to get to:] Therefore,  $Q$ . So  $P \Rightarrow Q$ , as required.

(b) Now we show that  $Q \Rightarrow P$ : assume  $Q$ . [Do some stuff in here to get to:] Therefore,  $P$ . So  $Q \Rightarrow P$ , as required.

Since  $P \Rightarrow Q$  and  $Q \Rightarrow P$ , we conclude that  $P \Leftrightarrow Q$ . **ATWMR**

**Exercise C(i)-9.** Use the method outlined in Proposition C(i)-3 to show that an integer  $n$  is divisible by 6 if, and only if,  $n$  is both even and divisible by 3. Hint for one of the directions: note that, if  $n$  is divisible by 3, then  $n = 3k$  for some integer  $k$ . Now if  $n$  is also divisible by 2 – that is, if  $n$  is even – what does the equation  $n = 3k$  tell you about  $k$ ? Use Exercise C(i)-1(b).

*Remark.* An “if and only if” proof can sometimes be shortened by observing that each step in the proof not only is implied by, but also implies, the previous one. For example, consider the following:

**Proposition C(i)-3<sub>E</sub>.**  $n$  is an even number if and only if  $n - 1$  is an odd number.

*Proof.*  $n$  is even iff  $n = 2k$  for some integer  $k$ , which is true iff  $n - 1 = 2k - 1$  for some integer  $k$ , which is true iff  $n - 1$  is odd.

So  $n$  is even iff  $n - 1$  is odd. **ATWMR**

**Exercise C(i)-10.** Let  $x$  be a real number. Use the method of proof shown in Proposition C(i)-3<sub>E</sub> to show that  $x^2 = 1$  iff  $x = -1$  or  $x = 1$ . (Pretend you didn't know this already.) Hint:  $x^2 = 1$  iff  $x^2 - 1 = 0$ . Now factor  $x^2 - 1$ , and use the fact that, for  $a, b$  real numbers, the product  $ab$  equals zero iff  $a = 0$  or  $b = 0$  (or both).

### Part C(ii): $A \subseteq B$ and related results

As a nice illustration of what can be done with the idea of  $P \Rightarrow Q$ , we consider the statement  $A \subseteq B$ . Here  $A$  and  $B$  are sets; the statement  $A \subseteq B$  is read “ $A$  is a subset of  $B$ ,” which just means  $A$  is *contained* in  $B$ , which just means every element of  $A$  is also an element of  $B$ , which just means  $P \Rightarrow Q$ , where  $P$  is the statement “ $x \in A$ ” and  $Q$  the statement “ $x \in B$ .” (The symbol “ $\in$ ” is read “is an element of.”) So an “ $A \subseteq B$ ” result *is* a “ $P \Rightarrow Q$ ” result, of a certain kind.

**Proposition C(ii)-1.**  $A \subseteq B$ .

*Proof.* Let  $x \in A$ . [Now do what you've got to, to get to:] Therefore,  $x \in B$ .

So  $A \subseteq B$ . **ATWMR**

As an easy, but illustrative, example, let's recall that, for general sets  $S$  and  $T$ ,  $S \cap T$  means the set of all objects that belong to  $S$  *and* belong to  $T$ . Then:

**Proposition C(ii)-1<sub>E</sub>.** For any sets  $S$  and  $T$ , we have  $S \cap T \subseteq S$ .

*Proof.* Let  $x \in S \cap T$ . Then  $x \in S$  and  $x \in T$ , so in particular,  $x \in S$ . So  $S \cap T \subseteq S$ . **ATWMR**

**Exercise C(ii)-1.** Show that the set of all integer multiples of 4 is contained in the set of all even numbers.

**Exercise C(ii)-2.** Show that the set of all perfect fourth powers is contained in the set of all perfect squares. (A perfect fourth power is an integer  $m$  such that  $m = \ell^4$  for some integer  $\ell$ ; similarly we define perfect squares.)

For the next two exercises, recall that, for sets  $S$  and  $T$ ,  $S \cup T$  denotes the union of  $S$  and  $T$ , meaning the set of all things in  $S$  or in  $T$ .

*Remark.* In mathematics, the word “or” is always, unless otherwise specified, used in the *inclusive* sense. That is, a mathematical statement of the form “ $X$  or  $Y$ ” will always, unless otherwise stated, mean “ $X$  or  $Y$  or *both*.” In particular,  $S \cup T$  denotes the set of objects either in  $S$ , or in  $T$ , or perhaps in both. For example, {integer multiples of 3}  $\cup$  {integer multiples of 5} *includes* the number 45, since 45 is both a multiple of 3 *and* a multiple of 5.

**Exercise C(ii)-3.** Show that, for any sets  $S$  and  $T$ , we have  $S \subseteq S \cup T$ .

**Exercise C(ii)-4.** Show that, for any sets  $A$ ,  $B$ , and  $C$ , we have  $A \cap B \subseteq A \cup C$ .

Now two sets are, by definition, equal if each is contained in the other: so to *prove* two sets  $A$  and  $B$  are equal, it’s enough to prove that  $A \subseteq B$  and that  $B \subseteq A$ . Like this:

**Proposition C(ii)-2.**  $A = B$ .

*Proof.* (a) We first show that  $A \subseteq B$ : let  $x \in A$ . [Now go until you get to:] Therefore,  $x \in B$ . So  $A \subseteq B$ , as required.

(b) We now show  $B \subseteq A$ : let  $x \in B$ . [Now go until you get to:] Therefore,  $x \in A$ . So  $B \subseteq A$ , as required.

Since  $A \subseteq B$  and  $B \subseteq A$ , we have  $A = B$ . **ATWMR**

As a concrete example, let’s define the *symmetric difference*  $C \Delta D$  of sets  $C$  and  $D$  by

$$C \Delta D \stackrel{\text{def'n}}{=} (C - D) \cup (D - C).$$

(Recall: in general  $A - B$  means the set of all things in  $A$  but not in  $B$ .) We have:

**Proposition C(ii)-2<sub>E</sub>.**  $C \Delta D = (C \cup D) - (C \cap D)$ .

*Proof.* (a) We show  $C \Delta D \subseteq (C \cup D) - (C \cap D)$ : let  $x \in C \Delta D$ . By definition of  $C \Delta D$ , this means  $x \in C - D$  or  $x \in D - C$ . If  $x \in C - D$  then  $x \in C$ , so  $x \in C \cup D$ , but  $x \notin D$ , so  $x \notin C \cap D$ . Therefore  $x \in (C \cup D) - (C \cap D)$ . On the other hand, if  $x \in D - C$  then  $x \in D$ , so  $x \in C \cup D$ , but  $x \notin C$ , so  $x \notin C \cap D$ . Therefore  $x \in (C \cup D) - (C \cap D)$ . So in either case  $x \in (C \cup D) - (C \cap D)$ . So  $C \Delta D \subseteq (C \cup D) - (C \cap D)$ , as required.

(b) We show  $(C \cup D) - (C \cap D) \subseteq C \Delta D$ : let  $x \in (C \cup D) - (C \cap D)$ . Then  $x \in C \cup D$  but  $x \notin C \cap D$ . Now since  $x \in C \cup D$ , we know  $x \in C$  or  $x \in D$ . If  $x \in C$  then, since  $x \notin C \cap D$ , we have  $x \notin D$ , so  $x \in C - D$ , whence  $x \in C \Delta D$  (by definition of  $C \Delta D$ ). If  $x \in D$  then, since  $x \notin C \cap D$ , we have

$x \notin C$ , so  $x \in D - C$ , whence  $x \in C \Delta D$  (by definition of  $C \Delta D$ ). So in either case  $x \in C \Delta D$ . So  $(C \cup D) - (C \cap D) \subseteq C \Delta D$ , as required.

Since  $C \Delta D \subseteq (C \cup D) - (C \cap D)$  and  $(C \cup D) - (C \cap D) \subseteq C \Delta D$ , we have  $C \Delta D = (C \cup D) - (C \cap D)$ .  
**ATWMR**

(Suggestion: draw a Venn diagram to understand symmetric differences and Proposition C(i)-5E.)

**Exercise C(ii)-5.** Let  $\mathbb{Z}$  denote the set of integers. Also, for given integers  $b$  and  $r$ , let  $b\mathbb{Z} + r$  denotes the set of all integers of the form  $bq + r$  for some integer  $q$ . (For example,  $7\mathbb{Z} + 3 = \{\dots, 7(-3) + 3, 7(-2) + 3, 7(-1) + 3, 7(0) + 3, 7(1) + 3, 7(2) + 3, 7(3) + 3, \dots\} = \{\dots, -18, -11, -4, 3, 10, 17, 24, \dots\}$ .)

Using the strategy of Proposition C(ii)-2, prove that

$$\mathbb{Z} = 3\mathbb{Z} \cup 3\mathbb{Z} + 1 \cup 3\mathbb{Z} + 2,$$

where  $3\mathbb{Z}$  is shorthand for  $3\mathbb{Z} + 0$ , and in general,  $A \cup B \cup C$  denotes the set of all objects either in  $A$ , or  $B$ , or  $C$ .

Hint: use the division algorithm, referenced at the top of p. 4 above, and on p. 29 of T-BOP.

**Exercise C(ii)-6.** Is the union  $3\mathbb{Z} \cup 3\mathbb{Z} + 1 \cup 3\mathbb{Z} + 2$  described in the previous problem *disjoint*? That is, do any two of the sets  $3\mathbb{Z}$ ,  $3\mathbb{Z} + 1$ , and  $3\mathbb{Z} + 2$  have any elements in common? Hint: think about the *uniqueness* described in the division algorithm.

**Exercise C(ii)-7.** Using the strategy of Proposition C(ii)-2, prove that, for any sets  $X$ ,  $Y$ , and  $Z$ ,

$$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z).$$

(It may help to draw a Venn diagram to help you understand what's going on here. But a Venn diagram does not suffice here for a *proof*.)

**Part C(iii):  $\forall x \in X, Q(x)$ ;  $\exists x \in X: Q(x)$ , and related results**

If  $Q(x)$  is a statement regarding a generic element  $x$  of a set  $X$ , then the statement " $\forall x \in X, Q(x)$ " means "for all  $x \in X$ ,  $Q(x)$  is true." Thus the " $\forall$ ," called the *universal quantifier*, means "for all."

The statements " $\forall x \in X, Q(x)$ ," "for any  $x \in X$ ,  $Q(x)$  is true," "given  $x \in X$ ,  $Q(x)$  is true," and "if  $x \in X$ , then  $Q(x)$  is true" all mean the same thing. In particular, the last statement is of the form  $P \Rightarrow Q$ . So, recalling part **C(i)** above, we have the following strategy for proving " $\forall x \in X, Q(x)$ :"

**Proposition C(iii)-1.**  $\forall x \in X, Q(x)$ .

*Proof.* Assume  $x \in X$ . [Now do what you got to, to get to:] Therefore,  $Q(x)$ .

So  $\forall x \in X, Q(x)$ . **ATWMR**

For example:

**Proposition C(iii)-1E.**  $\forall p \in \{\text{prime numbers}\} - \{3\}, 3 \text{ divides } p^2 + 2$ . [That is: if  $p$  is any prime number not equal to 3, then 3 divides  $p^2 + 2$ .]

*Proof.* Assume  $p$  is prime and not equal to 3. Then  $p$  is not divisible by 3 (a prime is only divisible by itself and 1), so if we divide 3 into  $p$  we get quotient  $k$  and a *nonzero* remainder  $r$ . Since  $r$  must be  $< 3$ , we have  $r = 1$  or  $r = 2$ . That is,  $p = 3k + r$  for some integer  $k$ , and  $r = 1$  or  $r = 2$ .

But note, then, that

$$p^2 + 2 = (3k + r)^2 + 2 = 9k^2 + 6kr + r^2 + 2 = 3(3k^2 + 2kr) + r^2 + 2. \quad (\circ)$$

If  $r = 1$  then  $r^2 + 2 = 3$ ; if  $r = 2$  then  $r^2 + 2 = 6$ ; in either case  $r^2 + 2$  is a multiple of 3. That is, in either case  $r^2 + 2 = 3m$  for some  $m$ . So  $(\circ)$  gives

$$p^2 + 2 = 3(3k^2 + 2kr + m),$$

which implies that  $p^2 + 2$  is a multiple of 3.

Therefore,  $\forall p \in \{\text{prime numbers}\} - \{3\}$ , 3 divides  $p^2 + 2$ . **ATWMR**

**Exercise C(iii)-1.** Prove that,  $\forall m \in \mathbb{Z}$ , the product  $m(m+1)(m+2)$  is divisible by 6.

**Exercise C(iii)-2.** Prove that,  $\forall x, y \in \mathbb{R}$  (recall that  $\mathbb{R}$  denotes the set of real numbers), we have

$$x^2 + y^2 \geq 6x + 4y - 15.$$

Hint: complete the squares. (Note: “ $\forall x, y \in \mathbb{R}$ ” means “if  $x \in \mathbb{R}$  and  $y \in \mathbb{R}$ .”)

We next consider the sentence “ $\exists x \in X : Q(x)$ ,” which means “for some  $x \in X$ ,  $Q(x)$  is true.” Thus the “ $\exists$ ,” called the *existential quantifier*, means “for some.”

The statements “ $\exists x \in X : Q(x)$ ,” “there is an  $x \in X$  such that  $Q(x)$  is true,” and “there’s at least one  $x \in X$  such that  $Q(x)$  is true” all mean the same thing. The most direct method of proving a statement like  $\exists x \in X : Q(x)$  is by *finding* an  $x \in X$  such that  $Q(x)$  holds. Such a proof is called *constructive*, and looks like this:

**Proposition C(iii)-2.**  $\exists x \in X : Q(x)$ .

*Proof.* Let  $x =$  [some element of  $X$  you’ve found that such that  $Q(x)$  holds. Then *show* that  $Q(x)$  holds, for this  $x$ , to conclude:] Then  $Q(x)$  holds.

So  $\exists x \in X : Q(x)$ . **ATWMR**

Remark on constructive proofs: generally, you *do not* need to show the work that went into *finding* the  $x$  that works. However, once you have produced this  $x$ , you do *show* that it works (that is, it makes  $Q(x)$  true).

**Proposition C(iii)-2E.**  $\exists k \in \{\text{numbers between 30 and 50}\} : k \text{ divides } 576$ .

*Proof.* Let  $k = 48$ . Then  $576 = 12k$ , so  $k$  divides 576.

So  $\exists k \in \{\text{numbers between 30 and 50}\} : k \text{ divides } 576$ . **ATWMR**

(The “work” that goes into finding the number  $k$  appropriate for the above proposition amounts simply to checking all numbers between 30 and 50 ’til one does the job. Again, in the proof you don’t show this work; you just present the result, and show that it *does* do the job.)

**Exercise C(iii)-3.** Prove that  $\exists p \in \{\text{prime numbers}\}$  such that  $p > 100$ .

**Exercise C(iii)-4.** Prove that  $\exists k \in \mathbb{Z}$  such that  $k$  can be expressed as a sum of two squares in two different ways. Hint: you don’t have to go too far; there’s a  $k < 100$  that works.



Quantifiers can be combined in various ways; for example, we can form statements like “ $\forall x \in X, \exists y \in Y: Q(x, y)$ .” We’ll consider a particularly useful context for such a combination in the next section. In the meantime, we note that great care should be taken with such combinations. In particular, the *order* of combination *matters*, as the following exercise attests.

**Exercise C(iii)-5. (a)** Prove that:

$$\forall x \in \mathbb{R}, \exists y \in \mathbb{R}: x > y.$$

**(b)** Prove that the statement

$$\exists y \in \mathbb{R}: \forall x \in \mathbb{R}, x > y$$

is false.

### Part C(iv): Quantifiers and limits

One area where quantifiers may be applied quite nicely is in the discussion of *limits*. Specifically: let

$$x_1, x_2, x_3, \dots$$

be a sequence of real numbers. Recall: to say

$$\lim_{n \rightarrow \infty} x_n = L \tag{*}$$

is, intuitively, to say that  $x_n$  gets closer and closer to  $L$  as  $n$  gets larger and larger. Or, somewhat more precisely: (\*) means we can make  $x_n$  as close as we want to  $L$ , by making  $n$  large enough. Or, even more precisely: (\*) means we can make  $|x_n - L|$  as small as we want, by making  $n$  large enough. Or, still *more* precisely, it means we can make  $|x_n - L|$  smaller than any prescribed positive tolerance, call it  $\varepsilon$ , by making  $n$  large enough, say bigger than some real number  $R$ .

In other (more mathematical) words, (\*) means: *for any  $\varepsilon > 0$ , there exists an  $R \in \mathbb{R}$  such that  $|x_n - L| < \varepsilon$  if  $n > R$ .*

So, in light of what we’ve discussed above concerning the phrases “for any,” “there exists,” and “ $Q$  if  $P$ ,” we are ready for:

**Definition C(iv)-1.** We say

$$\lim_{n \rightarrow \infty} x_n = L$$

if,  $\forall \varepsilon > 0, \exists R \in \mathbb{R}$  such that  $n > R \Rightarrow |x_n - L| < \varepsilon$ .

So that’s the definition. (It’s due to Cauchy, ca. 1827.) It does require some practice to get one’s brain around this definition, to the point of being able to *use* it to prove things.

To this end, let’s begin with a template for a limit proof.

**Proposition C(iv)-1.**

$$\lim_{n \rightarrow \infty} x_n = L.$$

*Proof.* Let  $\varepsilon > 0$ . [This is just shorthand for “Assume  $\varepsilon \in \{\text{positive real numbers}\}$ .”] Let  $R =$  [some expression involving  $\varepsilon$ : you’ve done work elsewhere to determine which  $R$  will work for you, but you don’t show that work here. The point is, to show existence of an appropriate  $R$ , you produce

it. In other words, your method of proof is constructive.] Assume  $n > R$ . Then [do what you have to do, to show that]  $|x_n - L| < \varepsilon$ . So  $\lim_{n \rightarrow \infty} x_n = L$ . **ATWMR**

Now let's work a couple of examples, to gain familiarity with the relevant ideas.

**Proposition C(iv)-1<sub>E</sub>.**

$$\lim_{n \rightarrow \infty} \frac{1}{n} = 0.$$

*Proof.* Let  $\varepsilon > 0$ . [What's in square-brackets here is what you might call scratch work: you wouldn't present it as part of your solution, but it's the kind of thing you'd be thinking to arrive at that solution. Now, we want  $R$  so that, if  $n > R$ , then  $|1/n - 0| < \varepsilon$ . The latter is the same as  $1/n < \varepsilon$ . Let's solve this for  $n$  to find how big  $n$  should be: certainly  $1/n < \varepsilon$  means  $n > 1/\varepsilon$ . So there you have it: let  $R = 1/\varepsilon$  and you're done. OK, now here's what we write.] Let  $\varepsilon > 0$  be given. Let  $R = 1/\varepsilon$ . If  $n > R$ , then  $|1/n - 0| = 1/n < 1/R = \varepsilon$ . So by Definition C(iv)-1,

$$\lim_{n \rightarrow \infty} \frac{1}{n} = 0,$$

as required. **ATWMR**

**Exercise C(iv)-1.** Show that

$$\lim_{n \rightarrow \infty} \frac{1}{\sqrt{n}} = 0.$$

Use only arguments involving  $\varepsilon$ 's and  $R$ 's, as in the proof of Proposition C(iv)-1<sub>E</sub> above. That is, you're not allowed to use limit laws like "the limit of the square roots is the square root of the limits" or what have you.

Here's another example.

**Proposition C(iv)-1<sub>EE</sub>.**

$$\lim_{n \rightarrow \infty} \frac{2n + (-1)^n}{n + 1} = 2.$$

*Proof.* [Scratch work: let  $\varepsilon > 0$ . We want  $R$  so that, if  $n > R$ , then

$$\left| \frac{2n + (-1)^n}{n + 1} - 2 \right| < \varepsilon.$$

But note that

$$\left| \frac{2n + (-1)^n}{n + 1} - 2 \right| = \left| \frac{2n + (-1)^n - 2(n + 1)}{n + 1} \right| = \left| \frac{(-1)^n - 2}{n + 1} \right| \leq \frac{1 + 2}{n + 1} = \frac{3}{n + 1} < \frac{3}{n}.$$

(We used the triangle inequality to get  $|(-1)^n - 2| \leq |(-1)^n| + |-2| = 1 + 2 = 3$ .) If we can make  $3/n < \varepsilon$  then we'll be done: but note  $3/n < \varepsilon \Leftrightarrow n/3 > 1/\varepsilon \Leftrightarrow n > 3/\varepsilon$ . OK, now here's what we write.] Let  $\varepsilon > 0$  be given. Let  $R = 3/\varepsilon$ . If  $n > R$ , then

$$\begin{aligned} \left| \frac{2n + (-1)^n}{n + 1} - 2 \right| &= \left| \frac{2n + (-1)^n - 2(n + 1)}{n + 1} \right| = \left| \frac{(-1)^n - 2}{n + 1} \right| \leq \frac{1 + 2}{n + 1} = \frac{3}{n + 1} \\ &< \frac{3}{n} < \frac{3}{3/\varepsilon} = \varepsilon. \end{aligned}$$

So by Definition C(iv)-1,

$$\lim_{n \rightarrow \infty} \frac{2n + (-1)^n}{n + 1} = 2,$$

as required. **ATWMR**

**Exercise C(iv)-2.** Show that

$$\lim_{n \rightarrow \infty} \frac{n^2 + (-1)^n n}{3n^2 + 1} = \frac{1}{3}.$$

The same rules apply as in Exercise C(iv)-1. HINT: Show that

$$\left| \frac{n^2 + (-1)^n n}{3n^2 + 1} - \frac{1}{3} \right| \leq \frac{3n + 1}{3(3n^2 + 1)}.$$

Since  $1 \leq n$  by assumption, the latter is  $\leq 4n/(3(3n^2 + 1)) < 4n/(3(3n^2)) = 4/(9n)$ . Now proceed similarly to the proof of Proposition C(iv)-1<sub>EE</sub>.

**Exercise C(iv)-3.** Show that

$$\lim_{n \rightarrow \infty} \frac{4n^3 + n + \sin n}{7n^3 + 3} = \frac{4}{7}.$$

The same rules apply as in Exercises C(iv)-1 and C(iv)-2.

We can prove most of the usual, familiar **limit laws** using Definition C(iv)-1 above. For example:

**Proposition C(iv)-1<sub>EEE</sub>.**

$$\lim_{n \rightarrow \infty} (x_n + y_n) = \lim_{n \rightarrow \infty} x_n + \lim_{n \rightarrow \infty} y_n,$$

providing both limits on the right hand side exist.

*Proof.* Let's write

$$\lim_{n \rightarrow \infty} x_n = L \quad \text{and} \quad \lim_{n \rightarrow \infty} y_n = M. \quad (**)$$

Let  $\varepsilon > 0$ . [Scratch work: we want to find  $R$  so that  $n > R \Rightarrow |x_n + y_n - (L + M)| < \varepsilon$ . But note, by the triangle inequality on  $\mathbb{R}$ ,

$$|x_n + y_n - (L + M)| = |(x_n - L) + (y_n - M)| < |x_n - L| + |y_n - M|.$$

If we pick  $R$  large enough to make each of the terms  $|x_n - L|$  and  $|y_n - M|$  smaller than  $\varepsilon/2$  – and we *can* do this, by Definition C(iv)-1 and (\*\*) – then we have the desired inequality. OK, here's what we write.] By (\*\*) and Definition C(iv)-1, we can choose an  $R_1$  such that  $n > R_1 \Rightarrow |x_n - L| < \varepsilon/2$ , and an  $R_2$  such that  $n > R_2 \Rightarrow |y_n - M| < \varepsilon/2$ . Let  $R = \max\{R_1, R_2\}$ : then

$$n > R \Rightarrow n > R_1 \text{ and } n > R_2 \Rightarrow |x_n + y_n - (L + M)| \leq |x_n - L| + |y_n - M| < \varepsilon/2 + \varepsilon/2 = \varepsilon.$$

So by Definition C(iv)-1,

$$\lim_{n \rightarrow \infty} (x_n + y_n) = L + M = \lim_{n \rightarrow \infty} x_n + \lim_{n \rightarrow \infty} y_n,$$

as required. **ATWMR**

**Exercise C(iv)-4.** Prove that, if  $C \in \mathbb{R}$ , then

$$\lim_{n \rightarrow \infty} Cx_n = C \lim_{n \rightarrow \infty} x_n,$$

providing the limit on the right exists.

The following limit law is a bit harder to prove.

**Proposition C(iv)-1EEEE.**

$$\lim_{n \rightarrow \infty} x_n y_n = \left( \lim_{n \rightarrow \infty} x_n \right) \left( \lim_{n \rightarrow \infty} y_n \right),$$

providing both limits on the right exist.

*Proof.* Let's call the limits on the right  $L$  and  $M$ , as in (\*\*). Let  $\varepsilon > 0$ . [Scratch work: we want to find  $R$  so that  $n > R \Rightarrow |x_n y_n - LM| < \varepsilon$ . The trick is as follows: write  $|x_n y_n - LM| = |x_n y_n - x_n M + x_n M - LM|$  and note, by the triangle inequality on  $\mathbb{R}$ , that

$$|x_n y_n - x_n M + x_n M - LM| \leq |x_n y_n - x_n M| + |x_n M - LM| = |x_n| |y_n - M| + |M| |x_n - L|.$$

By Definition C(iv)-1, we can pick  $n$  large enough to make  $|x_n - L| < \varepsilon/(2(|M|+1))$  and  $|y_n - M| < \varepsilon/(2(|L|+1))$ . (It's important to have an  $|M|+1$  and an  $|L|+1$  in the denominators, rather than just an  $|M|$  and  $|L|$ , since  $M$  or  $L$  could conceivably be zero and we want to avoid dividing by zero.) We can also, for  $n$  large enough, assure that  $|x_n| < |L|+1$ , because  $\lim_{n \rightarrow \infty} x_n = L$ , meaning for  $n$  large enough we have  $|x_n - L| < 1$  (we're just applying Definition C(iv)-1, with  $\varepsilon = 1$ ): but  $|a - b| \geq |a| - |b|$  always, so for  $n$  large enough  $|x_n| - |L| < 1$ , so  $|x_n| < |L| + 1$ . Now it may not be clear why we are bounding the various quantities involved in the indicated ways, but it will be once we write our proof. So here's what we write.] By (\*\*) and Definition C(iv)-1, we can choose an  $R_1$  such that  $n > R_1 \Rightarrow |x_n - L| < \varepsilon/(2(|M|+1))$ , an  $R_2$  such that  $n > R_2 \Rightarrow |y_n - M| < \varepsilon/(2(|L|+1))$ , and  $R_3$  such that  $n > R_3 \Rightarrow |x_n| < |L| + 1$ . Let  $R = \max\{R_1, R_2, R_3\}$ : then

$$\begin{aligned} n > R &\Rightarrow n > R_1 \text{ and } n > R_2 \text{ and } n > R_3 \\ &\Rightarrow |x_n y_n - LM| = |x_n y_n - x_n M + x_n M - LM| \leq |x_n y_n - x_n M| + |x_n M - LM| \\ &= |x_n| |y_n - M| + |M| |x_n - L| < (|L| + 1) \frac{\varepsilon}{2(|L| + 1)} + |M| \frac{\varepsilon}{2(|M| + 1)} \\ &< \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon. \end{aligned}$$

So by Definition C(iv)-1,

$$\lim_{n \rightarrow \infty} x_n y_n = LM = \left( \lim_{n \rightarrow \infty} x_n \right) \left( \lim_{n \rightarrow \infty} y_n \right),$$

as required. **ATWMR**

**Exercise C(iv)-5.** Prove that, if

$$\lim_{n \rightarrow \infty} x_n = L$$

and  $L > 0$ , then the  $x_n$ 's are “eventually” positive, meaning there is a real number  $R$  such that  $n > R \Rightarrow x_n > 0$ . Hint: let  $\varepsilon = L/2$ : by Definition C(iv)-1, there is a real number  $R$  such that  $n > R \Rightarrow |x_n - L| < L/2$ . What does this tell you about  $x_n$  itself in terms of  $L/2$ ?

**Exercise C(iv)-6.** Prove that

$$\lim_{n \rightarrow \infty} \sqrt{x_n} = \sqrt{\lim_{n \rightarrow \infty} x_n},$$

providing the limit on the right exists and is  $> 0$ . Hints: first you need an  $R_1$  such that  $n > R_1 \Rightarrow x_n > 0$  (use Exercise C(iv)-5), so that you can even consider the square roots on the left. Then, given  $\varepsilon > 0$ , you need an  $R_2$  such that  $n > R_2 \Rightarrow |\sqrt{x_n} - \sqrt{L}| < \varepsilon$ , where  $L = \lim_{n \rightarrow \infty} x_n$ . To achieve the latter, use the fact that

$$\sqrt{a} - \sqrt{b} = \frac{a - b}{\sqrt{a} + \sqrt{b}}$$

for  $a, b > 0$ . Now let  $R = \max\{R_1, R_2\}$ , and go for it.

*Remark.* Exercise C(iv)-6 exemplifies a more general limit law, namely: if  $\lim_{n \rightarrow \infty} x_n = L$  and  $f$  is *continuous* at  $x = L$ , then

$$\lim_{n \rightarrow \infty} f(x_n) = f(L).$$

Indeed, this is essentially the (or at least a) definition of continuity.

Next, we have the following HUGELY powerful limit law.

**Proposition C(vi)-1EEEE: The Squeeze Law.** If

$$x_n \leq y_n \leq z_n \tag{†}$$

for all  $n$  sufficiently large (meaning for all  $n$  larger than some fixed number  $R_1$ ), and

$$\lim_{n \rightarrow \infty} x_n = L = \lim_{n \rightarrow \infty} z_n,$$

then

$$\lim_{n \rightarrow \infty} y_n = L$$

as well.

*Proof.* let  $R_1$  be large enough that (†) holds for  $n > R_1$  (such an  $R$  exists by assumption). Let  $\varepsilon > 0$ . By Definition C(iv)-1 there is an  $R_2$  such that  $n > R_2 \Rightarrow |x_n - L| < \varepsilon$ , and an  $R_3$  such that  $n > R_3 \Rightarrow |z_n - L| < \varepsilon$ . But note  $|x_n - L| < \varepsilon \Rightarrow -\varepsilon < x_n - L \Rightarrow L - \varepsilon < x_n$ ; similarly  $|z_n - L| < \varepsilon \Rightarrow z_n - L < \varepsilon \Rightarrow z_n < L + \varepsilon$ . let  $R = \max\{R_1, R_2, R_3\}$ . Then by (†),

$$n > R \Rightarrow n > R_1 \text{ and } n > R_2 \text{ and } n > R_3 \Rightarrow L - \varepsilon < x_n \leq y_n \leq z_n < L + \varepsilon.$$

So  $n > R \Rightarrow L - \varepsilon < y_n < L + \varepsilon$ ; the latter is the same as  $|y_n - L| < \varepsilon$ . So by Definition C(iv)-1,

$$\lim_{n \rightarrow \infty} y_n = L,$$

as required. **ATWMR**

**Exercise C(iv)-7.** Prove the following **Lemma** (a “lemma” is a small result preceding, and used in the proof of, a larger one):

$$\lim_{n \rightarrow \infty} x_n = L \Leftrightarrow \lim_{n \rightarrow \infty} |x_n - L| = 0.$$

(This follows quite directly from Definition C(iv)-1.)

The result of Exercise C(iv)-7 is quite useful; for example, we use it in the following:

**Proposition C(iv)-1<sub>EEE</sub> revisited.**

$$\lim_{n \rightarrow \infty} (x_n + y_n) = \lim_{n \rightarrow \infty} x_n + \lim_{n \rightarrow \infty} y_n,$$

providing both limits on the right hand side exist.

*Proof.* We’ve already proved this, but this time, we do so using the squeeze law instead of  $\varepsilon$ ’s and  $R$ ’s. Here’s how: For all  $n \geq 1$  we have, by the triangle inequality,

$$0 \leq |x_n + y_n - (L + M)| \leq |x_n - L| + |y_n - M|. \quad (\square)$$

By assumption and the above lemma, the right side of  $(\square)$  goes to zero as  $n \rightarrow \infty$ ; certainly the left side does too. By the squeeze law  $|x_n + y_n - (L + M)| \rightarrow 0$  as  $n \rightarrow \infty$ , so by Exercise C(iv)-7,

$$\lim_{n \rightarrow \infty} (x_n + y_n) = L + M,$$

as required. **ATWMR**

The point is that, if one assumes the squeeze law, then one often does not need arguments that directly make use of  $\varepsilon$ ’s and  $R$ ’s.

**Exercise C(iv)-8.** Using the squeeze law instead of  $\varepsilon$ ’s and  $R$ ’s, prove that

$$\lim_{n \rightarrow \infty} \frac{3n + \cos n}{2n} = \frac{3}{2}.$$

Hint: get a common denominator to show that

$$0 \leq \left| \frac{3n + \cos n}{2n + 7} - \frac{3}{2} \right| \leq \frac{3}{2n}.$$

Now use the squeeze law, Exercise C(iv)-7, Proposition C(iv)-1<sub>E</sub>, and Exercise C(iv)-4.

**Exercise C(iv)-9.** Using the squeeze law instead of  $\varepsilon$ ’s and  $R$ ’s, re-prove the result of Exercise C(iv)-4.

There are MANY MANY other “ $\varepsilon$ - $R$ ” proofs that can be done *without* the  $\varepsilon$ ’s and the  $R$ ’s, if one has the squeeze law at one’s disposal. Of course the proof of the squeeze law *does* require  $\varepsilon$ ’s and  $R$ ’s, so the power of the squeeze law does *not* diminish, but in fact illuminates, the value of  $\varepsilon$ - $R$  proofs.

### Part C(v): Mathematical Induction

Suppose you want to show that a certain statement is true for any positive integer  $n$ . For example you might want to prove that, given any positive integer  $n$ ,

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2},$$

i.e. the sum of the first  $n$  positive integers is  $n(n+1)/2$ . Or you might want to show that, for any positive integer  $n$ ,

$$\int_0^1 (-\ln t)^n dt = n!.$$

These seem like pretty hard things to prove, since there are infinitely many positive integers and you only have a finite amount of time and patience.

Well, maybe you don't actually have to look at every integer  $n$ . It's sort of like dominoes: suppose you have an infinite line of dominoes, numbered consecutively as  $A_1, A_2, A_3, \dots$ , all standing on end. Also suppose:

- (a) The first domino  $A_1$  is knocked over, and
- (b) The dominoes are so arranged that each one, upon falling, will topple the next. That is, whenever the  $k$ th domino  $A_k$  falls, so will the  $(k+1)$ st domino  $A_{k+1}$ .

It's clear, at least intuitively, that from (a) and (b) you can conclude that all dominoes will eventually fall; that is, that the  $n$ th domino  $A_n$  will topple for any integer  $n$ . The principle of mathematical induction works in just the same way, except that instead of dominoes one has *mathematical assertions*. For example,  $A_n$  could be the assertion " $1 + 2 + 3 + \dots + n = n(n+1)/2$ ," or " $\int_0^1 (-\ln t)^n dt = n!$ ." We have:

**Principle C(v)-1: the principle of mathematical induction.** Let  $A_n$  be an assertion regarding a positive integer  $n$ . To prove that  $A_n$  is true for all  $n$ , it is enough to show:

- (Step 1)  $A_1$  is true,
- (Step 2) For any positive integer  $k$ ,  $A_k \Rightarrow A_{k+1}$ .

You don't need dominoes to understand the principle mathematical induction: think of it this way. Suppose you want to prove a statement  $A_n$  regarding an arbitrary positive integer  $n$ . If you can ascertain  $A_1$ , and that  $A_k$  gives you  $A_{k+1}$  for each positive integer  $k$ , then you can conceptually leapfrog from  $A_1$  to  $A_2$ , and then from  $A_2$  to  $A_3$ , and then from  $A_3$  to  $A_4$ , and so on until you conclude  $A_n$ . Step 1 of mathematical induction gives you your starting point; Step 2 allows you to make all of the jumps (in your head, you make them all at once).

So we can rewrite Principle C(v)-1, as a model **proof** by mathematical induction:

**Proposition C(v)-1.** For any positive integer  $n$ ,  $A_n$  is true.

*Proof.*

**Step 1.** [Prove  $A_1$ ]. So  $A_1$  is true.

**Step 2.** Assume  $A_k$ . [Then do what you need to do, to show that]: So  $A_{k+1}$  follows.

Therefore, by the principle of mathematical induction,  $A_n$  is true for all positive integers  $n$ .  
**ATWMR**

Step 1 is often called the "anchor" of a proof by mathematical induction. Step 2 is called the "inductive step;" the hypothesis  $A_k$  is called the "induction hypothesis." And remember: for Step

2 you need not *prove* that  $A_k$  is true; only that *whenever  $A_k$  is true, so is  $A_{k+1}$* , or in other words, that  $A_k \Rightarrow A_{k+1}$ .

For example, let us use mathematical induction to prove:

**Proposition C(v)-1<sub>E</sub>.** The sum of the first  $n$  positive integers is  $n(n+1)/2$ .

*Proof.* We let  $A_n$  be the statement

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

**Step 1.** Is  $A_1$  is true? Yes, since  $1 = 1(1+1)/2$ .

**Step 2.** We need to show that  $A_k$  implies  $A_{k+1}$  for all positive integers  $k$ . The statement  $A_k$  is

$$1 + 2 + 3 + \cdots + k = \frac{k(k+1)}{2}.$$

Assume that this is true. We need to show that  $A_{k+1}$  follows; in other words that

$$1 + 2 + 3 + \cdots + (k+1) = \frac{(k+1)((k+1)+1)}{2} = \frac{(k+1)(k+2)}{2}.$$

Let's examine the left-hand side of  $A_{k+1}$ . We have

$$\begin{aligned} 1 + 2 + 3 + \cdots + (k+1) &= (1 + 2 + 3 + \cdots + k) + (k+1) \\ &= \frac{k(k+1)}{2} + (k+1) = \frac{k(k+1) + 2(k+1)}{2} = \frac{(k+1)(k+2)}{2}, \end{aligned} \quad (1)$$

the second equality following from the induction hypothesis. But equation (1) is just the assertion  $A_{k+1}$ .

We have shown that  $A_1$  is true, and that  $A_k$  implies  $A_{k+1}$  for all positive integers  $k$ . By the principle of mathematical induction, we have proved that

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

for all positive integers  $n$ . **ATWMR**

Note that the *key step* in the above was equation (1), where we used  $A_k$  to deduce  $A_{k+1}$ . In particular, in equation (1), we: first wrote down the left-hand side of  $A_{k+1}$ , then did some algebra to express this in terms of the left-hand side of  $A_k$ , then used the induction hypothesis to rewrite this in terms of the *right-hand side* of  $A_k$ , then did some algebra to express this in terms of the right-hand side of  $A_{k+1}$ . This is often the kind of strategy that will work in a proof by mathematical induction.

**Exercise C(v)-1.** Use mathematical induction to prove that, for any positive integer  $n$ ,

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$



**Exercise C(v)-2.** Use mathematical induction to prove that, for any positive integer  $n$ ,

$$1 + 3 + 5 + 7 + \cdots + 2n - 1 = n^2.$$

That is: the sum of the first  $n$  consecutive *odd* positive integers is  $n^2$ .

**Exercise C(v)-3.** Use mathematical induction to prove that, for any positive integer  $n$ ,

$$\frac{d}{dx}x^n = nx^{n-1}$$

(pretend you didn't already know this, although it's OK to assume it's true for  $n = 1$ ). Hint: for the inductive step, use the product rule.

**Exercise C(v)-4.** [For students who have had second semester Calculus.] Use mathematical induction to prove that, for any positive integer  $n$ ,

$$\int_0^1 (-\ln x)^n dx = n!.$$

Hints: (a) note that this is an improper integral (since  $\ln x \rightarrow -\infty$  as  $x \rightarrow 0^+$ ); (b) use integration by parts.

**Exercise C(v)-5.** Use mathematical induction to prove that, for any positive integer  $n$ , the product of any  $n$  integers of the form  $4m + 1$  (where  $m$  is an integer) is itself of the form  $4m + 1$ .

**Exercise C(v)-6.** Let  $A_n$  be the statement

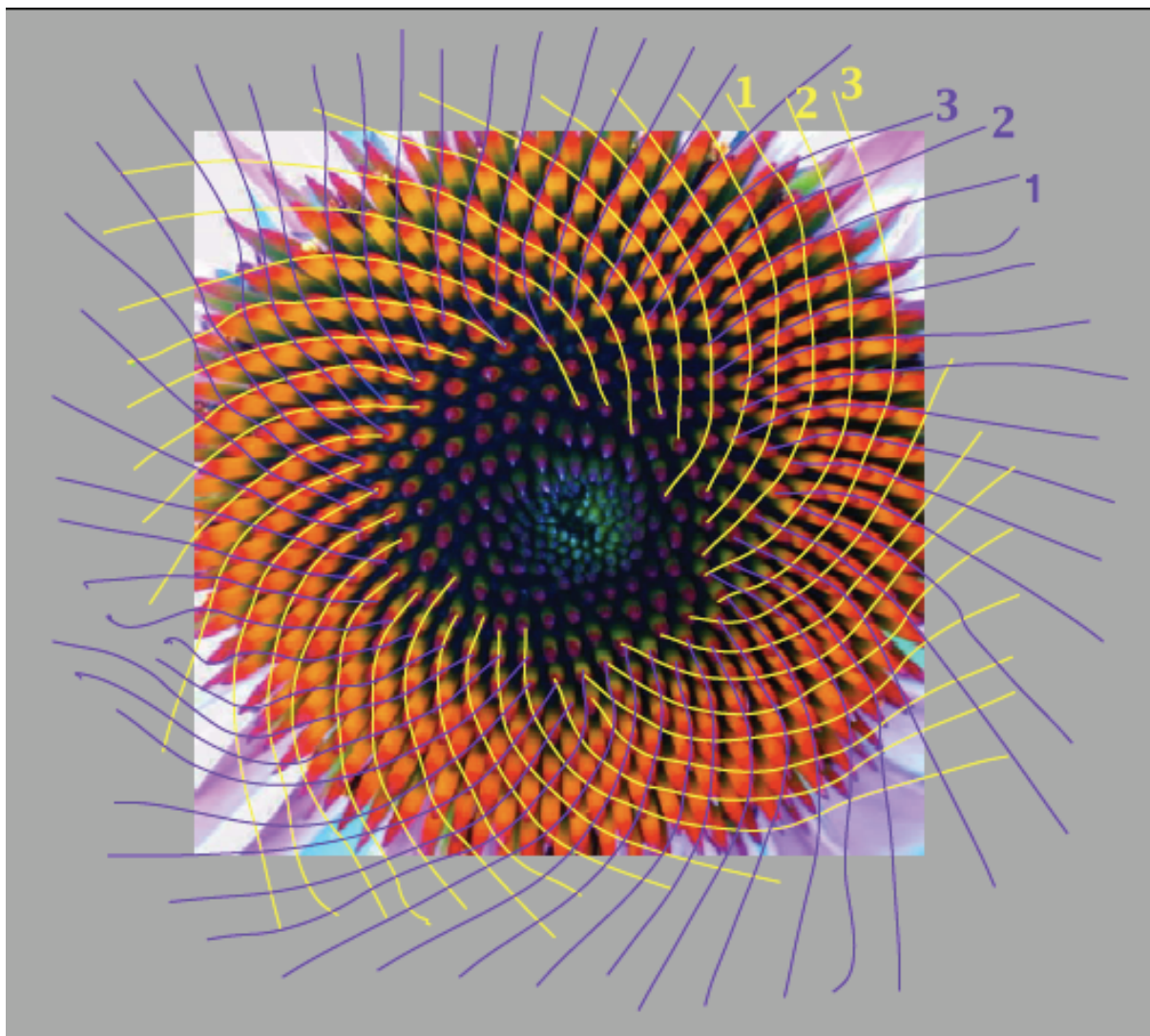
$$1 + 2 + 3 + \cdots + n = \frac{(2n+1)^2}{8}.$$

Prove that if  $A_k$  is true for any positive integer  $k$ , then so is  $A_{k+1}$ . Is  $A_n$  true for all positive integers  $n$ ? Explain your answer.

*Remark.* The principle of mathematical induction, while entirely plausible and perhaps even “obvious,” is in fact dependent on the *well-ordering principle*, a deep fact that we have already mentioned in connection with the division algorithm. See p. 4 above, and pp. 29-30 of T-BOP.

### Part C(vi): More on induction: Fibonacci numbers

**Exercise C(vi)-1.** Count the number of clockwise (yellow) and counterclockwise (purple) spirals in the coneflower below.



Clockwise spirals: \_\_\_\_\_ Counterclockwise spirals: \_\_\_\_\_

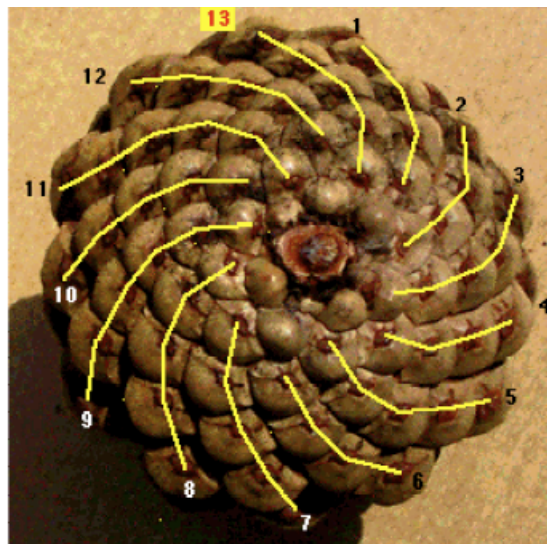
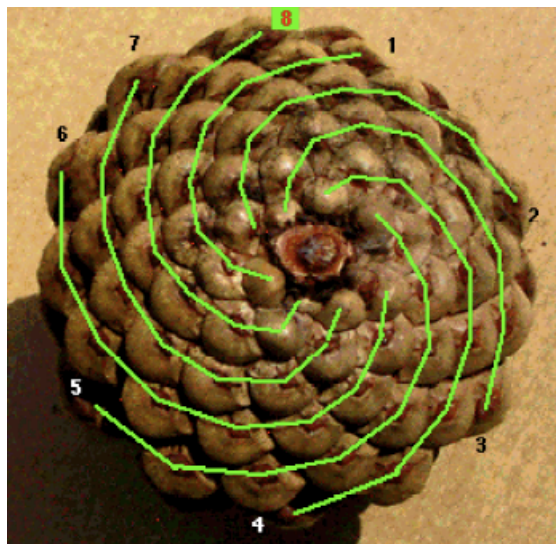
What's the significance of Exercise C(vi)-1? To answer, we define the *Fibonacci sequence*  $F_n$ , which looks like this:

$$1, 1, 2, 3, 5, 8, 13, 21, \dots$$

The rule for finding terms in this sequence is: the first term is 1; the second term is 1; to get any other term, add together the previous two terms. That is:  $F_1 = F_2 = 1$ ;  $F_{n+2} = F_{n+1} + F_n$  for  $n \geq 1$ .

**Exercise C(vi)-2.** Write down the nine Fibonacci numbers (that is, the nine terms in the Fibonacci sequence) that come right after the last Fibonacci number listed above.

FACT: Fibonacci numbers are EVERYWHERE. See, for example, Exercise C(vi)-1 above. Similarly, count clockwise and counterclockwise spirals on a pine cone: you'll get consecutive Fibonacci numbers! Really!!



Similar things happen with sunflowers, pineapples, broccoli florets, etc. See

[https://en.wikipedia.org/wiki/Fibonacci\\_number](https://en.wikipedia.org/wiki/Fibonacci_number)

Fibonacci numbers satisfy many curious relations. Here's one.

**Exercise C(vi)-3.** Using the principle of mathematical induction, prove that

$$F_{n+3}F_n - F_{n+1}F_{n+2} = (-1)^n.$$

Hint: If the above statement is  $A_n$ , then  $A_{k+1}$  is the statement

$$F_{k+4}F_{k+1} - F_{k+2}F_{k+3} = (-1)^{k+1}.$$

To see how this can be obtained from  $A_k$ , rewrite  $F_{k+4}$  and  $F_{k+2}$ , in the above statement of  $A_{k+1}$ , using the fact that a given Fibonacci number equals the sum of its two predecessors.

Particularly interesting things happen when we examine *ratios* of successive Fibonacci numbers. Let's do this.

**Exercise C(vi)-4.** Define a sequence  $R_n$  by

$$R_n = \frac{F_{n+1}}{F_n}$$

for  $n \geq 1$  ( $F_n$  denotes the  $n$ th Fibonacci number, as above). So the sequence  $R_n$  starts like this:

$$\frac{1}{1}, \frac{2}{1}, \frac{3}{2}, \frac{5}{3}, \frac{8}{5}, \frac{13}{8}, \dots$$

Write down the next nine  $R_n$ 's as fractions. Then write these nine terms as decimal numbers, with at least 4 places after the decimal point. Do the  $R_n$ 's appear to be converging? That is, do

they appear to have a limit? If so, what (approximately) does this limit appear to be (to as many decimal places as you care to speculate)?

The number to which your above  $R_n$ 's converge is, actually, a number that shows up in various other places too.

In the next problem, we investigate one of those places.

**Exercise C(vi)-5.** Find a half-dozen single-switch switchplates, meaning this kind of thing:



around your home, at school, etc. (Avoid switchplates that have extra stuff like electrical outlets, or that have multiple switches, or non-rectangular shapes, etc.) Measure the height and width of each switchplate in millimeters. Then compute the *Proportion* of the switchplate, defined to be the ratio of the height (longer side) to width (shorter side). Do this for each of your six switchplates, and supply the relevant info below (if your computed answers have more than four digits after the decimal, it suffices to write down only the first four of these digits):

Height: \_\_\_\_\_ Width: \_\_\_\_\_ Proportion: \_\_\_\_\_

Height: \_\_\_\_\_ Width: \_\_\_\_\_ Proportion: \_\_\_\_\_

Height: \_\_\_\_\_ Width: \_\_\_\_\_ Proportion: \_\_\_\_\_

Height: \_\_\_\_\_ Width: \_\_\_\_\_ Proportion: \_\_\_\_\_

Height: \_\_\_\_\_ Width: \_\_\_\_\_ Proportion: \_\_\_\_\_

Height: \_\_\_\_\_ Width: \_\_\_\_\_ Proportion: \_\_\_\_\_

The average (mean) of the above six Proportions is: \_\_\_\_\_

**Exercise C(vi)-6.** The number  $(1 + \sqrt{5})/2$ , often called the *golden mean* or the *golden ratio*, and often denoted by  $\Phi$ , is special. It shows up in many real-life, and mathematical, situations. What are some such situations? To answer, plug this number into your calculator, and evaluate as a decimal to a few decimal places. How does what you get compare to some of the numbers above? See especially exercises C(vii)-3 and C(vii)-4.

*Remark.* The golden ratio  $\Phi$ , or numbers close to it, also show up when you divide your height by the height of your belly button; the height of your face (chin to crown) by the width of your face;

etc. (Try it!!) There's an awful lot of debate as to whether these phenomena are deeply significant or not. (Perhaps the debate itself makes them significant.)

Let's return to the study of Fibonacci numbers *per se*. We note that the formula  $F_{n+2} = F_{n+1} + F_n$  for these numbers is *recursive*; it expresses a given Fibonacci number in terms of previous ones. Recursive formulas, on their own, can be a bit of a pain, because you can only use them to figure out a given term if you have already worked out all terms coming *before* that given one. (To compute  $F_{n+2}$  you only need, on the surface, to know  $F_n$  and  $F_{n+1}$ , but of course, to know these latter two quantities you need to have computed  $F_{n-1}$  and  $F_{n-2}$ , and so on down the line.)

There are various methods that can sometimes be employed to turn recursive formulas into *closed* formulas. A closed formula for a sequence is one where each term  $a_n$  is expressed directly in terms of the integer  $n$ , and not in terms of  $a_{n-1}$ ,  $a_{n-2}$ , etc.

As it turns out, there *is* a convenient closed formula for Fibonacci numbers. We won't discuss the derivation of this formula, but we will state the formula, and *prove* that the formula is correct.

**Proposition C(vi)-1.** If  $F_n$  denotes the  $n$ th Fibonacci number, then

$$F_n = \frac{1}{\sqrt{5}} \left[ \left( \frac{1 + \sqrt{5}}{2} \right)^n - \left( \frac{1 - \sqrt{5}}{2} \right)^n \right].$$

Proving this proposition is quite straightforward, if one has the following generalization of the principle of mathematical induction.

**Principle C(vi)-1: the principle of “double whammy” mathematical induction, or DWMI.** Let  $A_n$  be an assertion regarding a positive integer  $n$ . To prove that  $A_n$  is true for all  $n$ , it is enough to show:

- (Step 1)  $A_1$  is true,
- (Step 2)  $A_2$  is true,
- (Step 3) Whenever  $A_k$  and  $A_{k+1}$  are true for a positive integer  $k$ , then so is  $A_{k+2}$ .

**Exercise C(vi)-7.** Come up with an interesting, convincing ANALOGY for DWMI. Something like our domino analogy for the original principle of mathematical induction, but that better suits the situation at hand. be creative!!

**Exercise C(vi)-8.** Use DWMI to prove Proposition C(vi)-1. Hint: it might be useful to note that

$$\left( \frac{1 \pm \sqrt{5}}{2} \right)^2 = \frac{1 \pm 2\sqrt{5} + \sqrt{5}^2}{4} = \frac{6 \pm 2\sqrt{5}}{4} = \frac{3 \pm \sqrt{5}}{2}.$$

**Exercise C(vi)-9.** Let  $R_n$  be the ratio defined in Exercise C(vi)-4. Prove that

$$\lim_{n \rightarrow \infty} R_n = \Phi$$

where, again,  $\Phi$  denotes the golden ratio,  $\Phi = \frac{1+\sqrt{5}}{2}$ . (You don't need to use fancy “ $\varepsilon$ - $R$ ” limit arguments, like those in Section C(iv) above, to do this. Just use standard calculus techniques.)

Does this confirm the observations you made based on numerical calculations you did in Exercise C(vi)-6?

### Part C(vii): Proof by contradiction

We’ve demonstrated various different ways of proving various types of statements. Note that any given statement may be amenable to more than one strategy of proof.

We now introduce one more proof strategy, namely, the strategy of *proof by contradiction*.

Here’s the big idea behind this strategy: suppose you want to prove a statement  $T$ . If the assumption of  $\sim T$  leads to an *absurdity*, meaning something that is logically impossible, then the assumption of  $\sim T$  must have been incorrect, whereby  $\sim(\sim T)$ , which is to say  $T$ , must follow.

The absurdity that one generally shoots for in a proof by contradiction is one of the form “ $V$  and  $\sim V$ ,” where  $V$  is *any statement whatsoever!!* Indeed a statement, regardless of its nature, cannot be true at the same time as its negation is, so “ $V$  and  $\sim V$ ” is always an absurdity.

In sum, the general idea is:

**Proposition C(vii)-1.**  $T$ .

*Proof.* Assume  $\sim T$ . [Then do some stuff to conclude:] Therefore,  $V$ .

[Then do some other stuff to conclude:] Therefore,  $\sim V$ .

Thus,  $V$  and  $\sim V$ . Contradiction. Therefore,  $T$ . **ATWMR**

Sometimes, either  $V$  or  $\sim V$  will be obvious. For example:

**Proposition C(vii)-1<sub>E</sub>.** There are no integers  $a$  and  $b$  with  $6a + 28b = 1$ .

*Proof.* Let  $T$  be the above statement. We assume  $\sim T$  to be true; that is, we assume that there *do* exist integers  $a$  and  $b$  with  $6a + 28b = 1$ . Now 2 divides 6 and 2 divides 28, so by Exercise C(i)-3 above, 2 divides  $6a + 28b$  for any integers  $a$  and  $b$ , so by the assumption  $\sim T$ , 2 divides 1, meaning 1 is even.

But 1 is odd. Contradiction. So our assumption  $\sim T$  must be false, so  $T$  is true. That is: there are no integers  $a$  and  $b$  with  $6a + 28b = 1$ . **ATWMR**

**Exercise C(vii)-1.** Use proof by contradiction to show that there are no integers  $a$  and  $b$  with  $6a + 21b = 1$ .

**Exercise C(vii)-2.** Use proof by contradiction to show that there are no integers  $a$  and  $b$  such that  $a$  and  $b$  are both odd, and  $a^2 + b^2$  is a perfect square. Hint: call the statement in question  $T$ . Assume not  $T$ . Conclude that  $c^2 - 2$  is divisible by 4. Then derive a contradiction using Exercise C(i)-2 above (and the division algorithm).

As a less simple example, we have:

**Proposition C(vii)-1<sub>EE</sub>.** There are infinitely many prime numbers.

*Proof.* Assume it is not the case that there are infinitely many prime numbers: that is, assume there are finitely many, say  $K$ , of them. Denote them by  $p_1, p_2, \dots, p_K$ , and let  $S = \{1, p_1, p_2, \dots, p_K\}$ .

Put  $M = p_1 p_2 \cdots p_K + 1$ , and let  $q$  be the largest element of  $S$  that divides  $M$ . (Certainly  $q$  is positive, since  $S$  contains 1.) Note that, since  $q$  is an element of  $S$ , it divides the product of all

elements of  $S$ : so  $q$  divides  $N = p_1 p_2 \cdots p_K$ . But any integer dividing two integers divides their difference, so  $q$  divides

$$M - N = (p_1 p_2 \cdots p_K + 1) - p_1 p_2 \cdots p_K = 1.$$

The only positive integer dividing 1 is 1, so  $q = 1$ . [The statement  $V$  is, in this case, “ $q = 1$ .”]

On the other hand  $M$ , being an integer, has a positive prime divisor  $p$  (every integer does). Since all positive primes are in  $S$ ,  $p \in S$ , and since  $p$  is prime,  $p > 1$ . But recall  $q$  is the *largest* element of  $S$  that divides  $M$ : so  $q \geq p$ , whence  $q > 1$ . Therefore,  $q \neq 1$ .

So  $q = 1$  and  $q \neq 1$ . Contradiction. So there are infinitely many prime numbers. **ATWMR**

**Exercise C(vii)-3.** Prove that there are infinitely many positive prime numbers of the form  $4\ell + 3$  (for  $\ell$  an integer). Hint: Assume this is not the case. That is, assume there are finitely many, say  $K$ , positive prime numbers of the form  $4\ell + 3$ . Denote them by  $p_1, p_2, \dots, p_K$ , and let  $S = \{1, p_1, p_2, \dots, p_K\}$ . Now put  $M = 4p_1 p_2 \cdots p_K - 1$ . Note that  $M$  is of the form  $4j + 3$ , for  $j$  an integer (why?) Now proceed in a manner similar to that of Proposition C(vii)-1<sub>EE</sub> above. At some point, you may want to use the result of Exercise C(v)-5.

*Remark.* Suppose  $V$  is some statement such that  $V \Rightarrow \sim V$  and  $\sim V \Rightarrow V$ . Well, note that either  $V$  or  $\sim V$  must be true. In the first case we can deduce  $\sim V$ , and in the second we can deduce  $V$ . In either case, we find  $V$  and  $\sim V$  are true.

IN OTHER WORDS: one way of arriving at the statement “ $V \Rightarrow \sim V$  and  $\sim V \Rightarrow V$ ” used in the proof of Proposition C(vii)-1 is to come up with some statement  $V$  such that  $V \Rightarrow \sim V$  and  $\sim V \Rightarrow V$ . The corresponding proof by contradiction will then look like this:

**Proposition C(vii)-2.**  $T$ .

*Proof.* Assume  $\sim T$ . Assume  $V$ . [Then do some stuff to conclude:] Therefore,  $\sim V$ .

Assume  $\sim V$ . [Then do some stuff to conclude:] Therefore,  $V$ .

In either case ( $V$  or  $\sim V$ ), we have  $V$  and  $\sim V$ . Contradiction. Therefore,  $T$ . **ATWMR**

For example, we have:

**Proposition C(vii)-2<sub>E</sub>.** The square of any real number is non-negative (that is,  $\geq 0$ ).

*Proof.* Let  $T$  be the statement of the proposition. Assume  $\sim T$ . That is, assume there is some real number  $b$  with

$$b^2 < 0.$$



To derive a contradiction to  $\sim T$ , we’re going to consider the statement  $V$ :  $b > 0$ . We’ll show that, if we assume  $\sim T$ , then  $V \Rightarrow \sim V$  and  $\sim V \Rightarrow V$ . This will tell us, as described above, that the assumption  $\sim T$  must have been false.

So assume  $V$ :  $b > 0$ . Then, since multiplying both sides of an inequality by a positive number preserves the direction of the inequality, we can multiply both sides of  $(\text{fish})$  by  $b^{-1}$  to get  $b < 0$ , which certainly implies  $b \leq 0$ . So  $\sim V$ .



Now assume  $\sim V: b \leq 0$ . Of course  $b$  can't be zero because of (🐟) (and the fact that  $0^2 = 0$ ), so  $b < 0$ . Then, since multiplying both sides of an inequality by a negative number reverses the direction of the inequality, we can multiply both sides of (🐟) by  $b^{-1}$  to get  $b > 0$ . So  $V$ .

In either case ( $b > 0$  or  $b \leq 0$ ), we have  $b > 0$  and  $b \leq 0$ . Contradiction. So the square of any real number is non-negative. **ATWMR**

We're not claiming that the contradiction method gives the *easiest* proof of Proposition C(vii)-2<sub>E</sub>. But it does give *a* proof, and one that illustrates the ideas behind Proposition C(vii)-2.

Our next exercise provides a perhaps meatier illustration and application of these ideas, and is enough to make your head spin. (If your head is spinning already, this exercise is enough to start it spinning in the opposite direction.)

To present this exercise, we recall a couple of mathematical ideas: first, for any sets  $X$  and  $Y$  (finite or not), we say  $X$  and  $Y$  are *equivalent* if there is a bijection (a one-to-one, onto function) from  $X$  to  $Y$ . (Equivalent sets are said to have the same *cardinality*. Very roughly, cardinality can be understood as a measure of the *size* of a set.)

Next: for any set  $X$ , the *power set*  $\mathcal{S}(X)$  is defined to be the set of all *subsets* of  $X$ .

We have:

**Exercise C(vii)-4.** Fill in the blanks below to prove the following proposition: no set is equivalent to its power set.

*Proof.* We want to prove  $T$ : no set is equivalent to its power set. So assume  $\sim$ \_\_\_\_\_, that is, suppose *some* set, call it  $X$ , *is* equivalent to its power set  $\mathcal{S}(X)$ . This means there is a one-to-one, onto function  $f$  from  $X$  to \_\_\_\_\_.

By definition of  $f$  we know that, for each element  $x$  of  $X$ ,  $f(x)$  belongs to  $\mathcal{S}(X)$ , so  $f(x)$  is a \_\_\_\_\_ of  $X$ . This subset might contain the element  $x$ , or it might not. Let's consider the cases where it doesn't. Specifically, let's consider the set  $B$  of all elements of  $X$  such that  $f(x)$  *does not* contain  $x$ . That is, let

$$B = \{x \in X : \text{_____} \notin f(x)\}. \quad (\text{🐝})$$

Since  $B$  is a subset of \_\_\_\_\_, we have  $B \in \mathcal{S}(X)$ , and therefore, since  $f$  takes  $X$  *onto*  $\mathcal{S}(X)$ , there is some  $y \in X$  with


$$f(y) = B. \quad (\text{🚗})$$

Consider the statement  $V: y \in B$ . We are going to show that, under the assumption  $\sim T$ , we have  $V \Rightarrow \sim V$  and  $\sim V \Rightarrow V$ . Then, as in Proposition C(vii)-2, we will have a \_\_\_\_\_ to the statement  $\sim T$ , and thus we will be able to conclude the statement \_\_\_\_\_, thereby proving our proposition.

So assume  $y \in B$ . By the definition (🐝) of  $B$ , this means  $y \notin f(y)$ . But again, by (🚗), we have  $f(y) = \text{_____}$ . So  $y \notin B$ .

Now assume  $y \notin B$ . By the definition (🐝) of  $B$ , this means  $y \in \text{_____}$ . But again, by



() , we have  $f(y) = B$ . So  $y \in B$ .

In either case ( $y \in B$  or \_\_\_\_\_), we have \_\_\_\_\_ and  $y \notin B$ . Contradiction. Therefore, no set is equivalent to its \_\_\_\_\_. **ATWMR**

Some closing words: in a proof by contradiction, make sure you indicate clearly the point at which the contradiction occurs: for example, in our proofs above we did so with the word “Contradiction.” As a synonym for this word, you might want to consider the phrase “Hah! I’ve run rings round you logically!,” as in the following proof by contradiction from a famous Monty Python skit (here, “MPGID” stands for “Monty Python Guy in Drag”):

MPGID #1: What’s that on the television then?

MPGID #2: Looks like a penguin.

MPGID #1: Perhaps it’s from the zoo.

MPGID #2: If it came from the zoo, it would have “Property of the zoo” stamped on it.

MPGID #1: They don’t stamp animals “Property of the zoo.” You can’t stamp a huge lion!

MPGID #1: They stamp them when they’re small.

MPGID #2: What happens when they molt?

MPGID #1: Lions don’t molt!

MPGID #2: No, but penguins do. **Hah! I’ve run rings round you logically!**

**Exercise C(vii)-5.** What proposition are the Monty Python people proving? Write up carefully the statement, and the proof by contradiction, of this proposition.