(1.1) – The Language of Math

Right now, hopefully, you are reading this set of notes. So far it hasn't been very heavy- a chapter title and two sentences separated by a period. There was a set of parenthases above to note the chapter number, and a dash to separate that parenthasis from the actual title. In the first sentence of this paragraph there were two commas, while the second sentence contained a hyphen. Maybe you thought these were well-constructed sentences, and maybe you even understand why all that punctuation is there in the first place. Either way, you were able to read and understand this self-referential paragraph and perhaps take some questionable meaning out of it.

Think about why that is.

It is because you have a basic comprehension of language, grammar, and syntax. To a pretty fair extent, you "get" why some words follow others, and why we place commas and periods where we do. Without this comprehension of how these things work, the previous paragraph would look like heiroglyphics or ink smudges on a piece of paper.

So you understand the English language and can read, which are two pretty important things if you plan on passing a college english course. They are also two very important things if you plan on passing a college math course. Math, like english, is a *language*, and like any language, comes with its own set of rules that you have to follow in order to understand it. You can think of certain letters or numbers used in equations as an alphabet, and the symbols that connect them as punctuation. You already do this subconsciously without realizing it.

Look at the mathematical statement:

$a^2 + b^2 = c^2$

You probably read that as "a squared plus b squared is equal to c squared". In all likelihood, that got you thinking about a right triangle, and you might have even placed the c on the hypotenuse in your mind. You recognized the symbols for equal and plus, and the superscript used to denote the power of a number. You even understood abstract representations for the sides of a triangle, namely a, b, and c. That says nothing for what the statement even *means*. Within seconds you had translated the math language into something you could work with, and the process was probably as natural as understanding the meaning of an octogal red sign that reads STOP.

The point of this chapter is to introduce you to some symbols that are widely used in many different branches of mathematics. Without an understanding of math's unique language, progress through more advanced courses will be impossible. Recognizing and interpreting the following symbols and concepts will be your first step in gaining mathematical maturity.

Sets

A SET is a collection of things. Those things can be numbers or letters or something more complicated, such as a group of other sets. Some examples of sets are:

The set of the days of the weeks, such as Monday, Tuesday, Wednesday, etc.
The set of integers from 1 to 10.
The set of people in your 220 class.
The set of candies in your Halloween bag.
The set of differentiable functions in $\mathbb{R}^2$

At this point, you need only recognize the nature of the set, not necessarily what it contains. In this chapter, we will discuss only oft-used sets of numbers, such as the Reals or Integers.

Here are some of the sets you will see most often:

$\mathbb{Z}$ - The Set of all Integers
$\mathbb{Z}^+$ - The Set of all Positive Integers
$\mathbb{R}$ - The Set of all Real Numbers
$\mathbb{R}/\{0\}$ - The Set of all Reals, Minus the number Zero
$\mathbb{Q}$ - The Set of all Rational Numbers
$\mathbb{N}$ - The Set of all Natural Numbers, or Counting Numbers
$\mathbb{C}$ - The Set of all Complex Numbers

At some point in your math life before this class, you encountered all of the above sets, save one. While you may be familiar, and even comfortable with these sets, it is always important to rigidly define what we are talking about when introducing a new concept in math. Some of these require no fancy explanations- for example, the set of integers consists of the numbers $\{.....-3,-2,-1,0,1,2,3.....\}$, while the set of positive integers is $\{1,2,3,4.....\}$. As for some of the others, they will be formally defined as need dictates by the text. Until then, I will test the student's knowledge by referring to them in questions at the end of certain sections.

Of course, there are other sets of numbers than the ones listed above. These, however, are sufficient for the work you will be attempting in Discrete Math. As stated, you have seen most of them before, the possible exception being $\mathbb{R}/\{0\}$. It may seem odd to take an entire set, only to remove just one element. You will see that restricting certain sets sometimes gives them a mathematical property they didn't previously possess.

Also of special note is the difference between the sets $\mathbb{Z}^+$ and $\mathbb{N}$. There is none. They are two different ways of naming the same set.

Note: If element x is a member of set S, we denote this by writing $x \in S$

Take a look at these statements, and determine which of the following are true.

1. $\frac{2}{5} \in \mathbb{R}$
2. $0 \in \mathbb{Z}^+$
3. $\mathbb{Q} \in \mathbb{R}$
4. $\pi \in \mathbb{C}$
5. $\sqrt{7} \notin \mathbb{Z}$
6. $\mathbb{R} \ni 10!$

Nothing terribly difficult here, but let's give some explanations:

1. TRUE. The set of all real numbers certainly contains fractions.
2. FALSE. The set of positive integers does not contain zero. Its smallest element is 1. While 0 is a non-negative integer, it is not positive.
3. FALSE. While the set of rational numbers is wholly contained within the set of real numbers, it is not a single element in the set of real numbers. This is not to say that the two sets do not share a relationship- a course in Set Theory would claim that one is a *subset* of the other. We will revisit this concept in chapter 3.
4. TRUE. Complex numbers are of the form $a+bi$, where a and b are real numbers. π is a real number, and in this case $b = 0$.

5. TRUE. The square root of 7 is not an integer, as it is approximately 2.6458.
6. TRUE. $10! = 3628800$, which is obviously a real number. Note that the inclusion symbol is reversed and yet it does not affect the truth value of the statement.

As stated earlier, these are just some of the different sets you will encounter as you work your way through the more difficult undergraduate math classes. More information about these sets will be given as necessary.

Proofs

Much of this course will consist of proving the various theorems you will come across as you learn more advanced math techniques. These theorems will be stated in one of two ways. The first way is to write out the statement in a complete english sentence such as:

"If the sum of two integers is odd, then one of the integers is odd and the other is even."

The other way is to cut out a few of the words by writing this in mathematical shorthand:

The sum of two integers is odd $\rightarrow$ *one of those integers is odd, the other is even*

That probably seemed unimpressive, but we have now introduced another symbol into our growing dictionary. Namely, the right arrow, or $\rightarrow$. As shown in the previous example, $\rightarrow$ replaces the words "if, then" in the statement of a proof. What it tells us is to use the information on the left side of the arrow to prove the stuff on right side of the arrow. Much in the same way, a left arrow $\leftarrow$ tells us to use the information on the right side of our statement to prove whatever is on the left side. Finally, there is the important "if and only if" proof, which is denoted by $\leftrightarrow$. Here is an example:

"x is equal to an odd number if and only if $x + 1$ is an even number".
is the same as.....
x *is odd* $\leftrightarrow$ $x + 1$ *is even*

The symbols that you have learned thus far are the first in a language that will grow as your knowlege of mathematics increases. We will introduce more such symbols as the text goes on, but for the purposes of this section, these will suffice.

EXERCISES

1. Determine whether the following statements are either true or false. Justify your answer.

   (a) $\sqrt{196} \in \mathbb{Z}^+$

   (b) $1.2\bar{3} \in \mathbb{Q}$

   (c) $\mathbb{C} \ni \mathbb{R}/\{0\}$

   (d) $e + \pi \in \mathbb{C}$

   (e) $\mathbb{Z} \subset \mathbb{R}/0 \subset \mathbb{R}$

   (f) $-\frac{-1}{7.2} \in \mathbb{Q}$

   (g) $\mathbb{N} \subseteq \mathbb{Z}^+$

2. Shorten the following statements using mathematical symbols where applicable.

   (a) If a number is even, the square of that number is even.

   (b) If the set of rational numbers is a subset of the reals, then one half is a real number.

   (c) A triangle is isosceles if it has two angles of the same degree measure.

   (d) Two numbers are relatively prime if and only if they have a greatest common divisor of 1.

   (e) Cancellation under an operation holds if you are in a group.

   (f) x squared is a rational number if x is a rational number.

3. Place a left, right, or double arrow to make the following statements true. If the statements are unconnected, explain why.

   (a) $p \in \mathbb{R}$ —— $p^2 \in \mathbb{Z}^+$

   (b) A quadrilateral has four equal angles —— A quadrilateral is a square

   (c) A number has a remainder of 3 when divided by 4 —— A number is divisible by 7

   (d) p divides ab —— p divides either a or b

   (e) p divides a and p divides b —— p divides $(ab)^2$

   (f) A regular polygon has external angles of 60° —— A polygon is a hexagon

(1.2) – Quantifiers

In the previous chapter, we covered a few of the symbols that represent different sets, and some simple notation pertaining to proof statements. Now we will expand this language to include something in math called a QUANTIFIER. A quantifier is pretty much what it sounds like- a way to denote how much of something we want to deal with. In particular, many math statements make use of two different kinds of quantifiers, called the EXISTENTIAL QUANTIFIER and the UNIVERSAL QUANTIFIER.

The Existential Quantifier ($\exists$) is translated as “There exists.....”
The Universal Quantifier ($\forall$) is translated as “For all.....”

So we have two more symbols to deal with, but no context in which to place them. Here are some examples of how quantifiers are used:

1. $\exists x \in \mathbb{Z} : x + 2 = 3$
2. $\forall p$ (p prime) : (p)(0)=0
3. $\exists a \in \mathbb{Z} : a^2 - \frac{3}{2}a + \frac{1}{2} = 0$
4. $\forall q \in \mathbb{N} : -q^2 \leq 0$

Whenever confronted with more complicated math statements such as the ones shown above, it is most important to translate them properly before attempting to determine their truth value. Here is how we interpret these four examples:

1. *There exists an x in the set of integers such that x+2=3.* Note that we use : as a replacement for the words ”such that”. This is a basic algebra statement, and of course it is true. The x does exist, and it is 1.
2. *For all p that are prime, p multiplied by 0 equals 0.* This is also true.
3. *There exists an a in the set of integers such that* $a^2 - \frac{3}{2}a + \frac{1}{2} = 0$. Another true statement..... aren’t they all?
4. *For all q in the set of natural numbers, negative q squared is less than or equal to 0.* Yes, this is also true for all possible values of q.

Those are some of the simplest examples of how to use quantifiers. Often you will be asked to prove certain statements, or to determine the truth value of statements involving quantifiers. Here are some examples:

ex: $\forall t \in \mathbb{R} : \sqrt{t} \in \mathbb{R}$

This statement is FALSE. Take -1. $\sqrt{-1} = i$, which is not an element in the set of all reals.

ex: $\exists r, s \in \mathbb{C} : r + s \in \mathbb{R}$

This statement is TRUE. For example, if $s = 2 + 3i$ and $r = 2 - 3i$, then $r + s = 4 \in \mathbb{R}$.

Let's look at the first example above. The question is why it ended up being false. This may seem obvious at first, because we easily came up with an integer for which its square root was not a real number. But was this enough to claim that the entire statement is false? The answer is yes- in order to prove that something is NOT true for all x, all we have to do is find ONE example for which it is not true. This is called a *counterexample*. The counterexample we found for the first example above was $t = -1$.

Our counterexample presents us with yet another question: How do we determine the negation of a statement that involves a quantifier? Given the statement $\forall t \in \mathbb{R} : \sqrt{t} \in \mathbb{R}$, we figured out that we needed to find only one t for which the statement failed. So, the negation of our statement is:

$\exists t \in \mathbb{R} : \sqrt{t} \notin \mathbb{R}$

Translated, this says, "There exists a t in the set of reals such that $\sqrt{t}$ is not in the set of reals."

So in general, to negate a statement that begins with a single universal quantifier, we switch to the existential quantifier and negate the result. In the same way, to negate a statement that begins with a single existential quantifier, we switch to the universal quantifier and negate the result. Referring to the example above, the negation of the statement $\exists r, s \in \mathbb{C} : r + s \in \mathbb{R}$ is:

$\forall r, s \in \mathbb{C} : r + s \notin \mathbb{R}$

This is, of course, translated as, "For all r and s in the set of complex numbers, $r + s$ is not an element in the set of real numbers."

When we say that we are "negating" these statements, it is important to note that we are actually taking the *inverse* of the original. This is only mentioned in the spirit of accuracy- for the duration of this course, the terms converse and inverse are only mentioned as examples of what NOT to do with proofs. This will become clearer in future chapters. Finally, note that our statements and their negations have different truth values- if the original statement is true, its negation is false and vice versa. Moreso, this is precisely the method by which you prove a mathematical statement untrue. Simply prove its negation to be true.

There are certain pitfalls inherent in finding negations of these statements. It is often tempting to assume that the inverse of a 'for all' statement involves the word 'none'. For example, students often reply that the negation of the statement, "All students like math" is "No students like math". It may seem as if these two sentences are negations of each other, but that isn't the case. Think of it this way: if you wanted to prove the statement, "All students like math" to be false, what is it that needs to be true? Does it need to be true that every student dislikes math? NO! In order for the statement to be false, the only necessary condition is that ONE student dislikes math. It cannot be true that every student in a class likes math and yet there is one who does not. Keep this idea in mind when attempting to negate mathematical statements that contain the phrase "for all".

We should look at a similar example when negating math statements involving "there exists". Think of how you might prove this statement false: "There exists one person in my Discrete Math class who can stay awake when the teacher starts lecturing." If we were to negate this statement, is it sufficient to say that there is one person who CANNOT stay awake? It is not. In order for the statement to be false, EVERY student must fall asleep while the teacher is lecturing. This is actually the case more often than not.

The rules for negating can be written explicitly with symbols.
$\sim \forall x = \exists \sim x$
$\sim \exists x = \forall \sim x$

These rules are called *DeMorgan's Laws for quantifiers.* And that name DeMorgan is one you should probably get used to- you will be seeing it in just about every single math class you take from here on out.

Nested Quantifiers

The hope is that you found our intial statements involving quantifiers simple enough to follow, because they are about to get way more complicated. The meanings of statements such as those in our previous examples were fairly straightforward and readily translatable. Now take statements such as these:

1. $\exists a \forall b : a + b = 0$

2. $\forall x \exists y : x + y = 0$

3. $\forall p, q\ \exists r : p^2 r + q^2 r = -1\ (p, q, r \in \mathbb{R})$

Whether or not you personally find them more difficult than previous examples to translate, there is no doubt that this is the case. For obvious reasons, when two quantifiers play off of each other, they are called *nested quantifiers.* As always, care should be taken in determining exactly what each statement is trying to convey. Once you have figured that out, it is time to determine whether it is true or false. Looking above, it might seem like examples 1 and 2 are identical in meaning, but of course that is not the case. As a matter of fact, one is a true statement and the other is false. But which is which? Before looking at the answer below, try to come to a conclusion on your own.

1. "*There exists an* a *for all* b *such that* $a + b = 0$" This statement is FALSE. It is claiming that there is a singular a that exists, and that particular a, when added to *every* possible b, will result in 0. This is simply not the case, as there is no one a that sums with more than one value of b to get to 0. Depending on what value you have chosen for b, your a will change. Contrast this with the following:

2. "*For every* x*, there exists a* y *such that* $x + y = 0$" This statement is TRUE. No matter what value you choose for x, you will be able to find a y such that the sum of the two is equal to 0. In this case, each and every x gets its own y. This is actually the well-known inverse property for addition.

3. "*For all* p *and* q*, there exists an* r *such that* $p^2 r + q^2 r = -1$" So each p and q has a corresponding r that will make the equation true. This is FALSE. If p and q are both 0, there is no r that will render the equation valid.

These examples once again bring into question how to negate statements involving quantifiers. For example, we knew the third question was false because *there exists* a pair p and q such that the statement was not true. Here are the negations of the three above statements, with translations:

1. $\nexists a : \forall b,\ a + b = 0$
   "*There exists no* a *such that for every* b*,* $a + b = 0$"

2. $\exists x \forall y, x + y \neq 0$
   "There exists an x such that for all y, $x + y \neq 0$"

3. $\exists p, q : \forall r, p^2r + q^2r = -1$
   "There exist p, q such that for all r, $p^2r + q^2r \neq -1$"

EXERCISES

1. Translate the following statements and determine whether or not they are true:
   (a) $\exists x : 3x = 2$
   (b) $\exists v, w \in \mathbb{Z} : vw^2 + v^2w = 1$
   (c) $\forall y \in \mathbb{R} : \frac{1}{y} \in \mathbb{R}$
   (d) $\exists p, q \in \mathbb{Z}^+ : \frac{p}{q} + \frac{q}{p} < 2$
   (e) $\forall n : n! \neq 2k + 1, k \in \mathbb{Z}$
   (f) $\exists x \geq 2 : x! = n^2$, $n \in \mathbb{Z}$
2. Write each of the following mathematical statements as an english sentence, and prove whether or not it is true.
   (a) $\exists x : x + 2 = 5$
   (b) $\forall y < 1 : y^2 = 7$
   (c) $\exists r, s : r^s = 0$
   (d) $\forall x \in \mathbb{Z} : 3x \in \mathbb{Z}$
   (e) $\forall p \exists q$ s.t. $pq = 1$
   (f) $\exists x \forall y \in \mathbb{R} : xy - y = 0$
3. Negate the following statements:
   (a) $\exists p : p^2 = 4$
   (b) $\forall x \in \mathbb{R} : x \in \mathbb{Q}$
   (c) $\exists\ y \in \mathbb{Z}^+ : y^2 < 0$
   (d) $\forall t, s : (\frac{t}{s})(\frac{s}{t}) = 1$
4. Translate the following statements containing nested quantifiers. Determine their truth value.

(a) $\forall x \exists y : \; xy = 2$

(b) $\exists s \forall t : \; s + t = t$

(c) $\exists s \forall t : \; s + t = 2t$

(d) $\forall g \exists h : g^2 = h$

(e) $\exists x \forall y, y \neq 0 : xy = 1$

5. Determine the truth value of each of the following:

(a) $\exists x : x + 2 = 3$

(b) $\forall x : x^2 \neq x + 20$

(c) $\forall x : x^2 \neq x - 20$

(d) $\forall p : p^3 > p^2$

(e) $\forall r \in \mathbb{Z} : \frac{1}{r} \centerdot r \in \mathbb{Z}$

(f) $\forall x \in \mathbb{R} : \sqrt{x} \in \mathbb{C}$

(g) $x, y \in \mathbb{R}, x^y \in \mathbb{R}$

(h) $\forall x, \exists y : x + y = 0$

(i) $\forall x, y \in \mathbb{R}, \exists z (z = \frac{x+y}{2})$

(j) $\exists x \in \mathbb{Z}^+$ s.t. $2x^3 = x^2$

(k) $\exists x, y \in \mathbb{Z}^+ : xy = 0$

(l) $\exists x, y \in \mathbb{C}^+ : x + y \in \mathbb{Z}^+$

(m) $\forall x \in (\mathbb{R}, \centerdot), \exists x^{-1}$

(n) $\exists x \forall y : x + y = 0$

(o) $\exists s \forall t : s^t \in \mathbb{Z}$

(p) $\exists x \forall y : y^2 + xy + 4 \geq 0$

(q) $\forall x, y > 0 : xy - y > -100$

(r) $\forall x, y \exists z : x + y > xyz$

(s) $\forall x > 1, x! \neq n^2 (n \in \mathbb{Z})$

In the previous two sections, we started to build a language by which we will interpret future problems and theorems. In this section, we define the concept of an operator (even though we have been using them in these notes) and introduce some less common operators that will be used later in this text.

(1.3) – Strange Operators and Other Mathematical Concepts

Definition- An **OPERATOR** is a mathematical process that, when applied to an element, allows us to derive another element.

You have dealt with operators your entire mathematical life. Examples would be addition, subtraction, square root, log, sin, etc. When an operator connects two different mathematical elements, we call it a *Binary Operator.* Operators are meaningless on their own- they require numbers or variables to act upon. A log by itself takes on no meaning; place a number after it and it yields a value.

Definition- If $n \geq 0, n!$, or **n FACTORIAL** is defined as the product of all positive integers less than or equal to n.

We define 0! to be equal to 1 so that future definitions won't get "messed up".
Now, you have certainly encountered this operator before, and it is something that you probably worked with a good deal in the past. It is important to master how factorials work in relation to each other, as we will need to multiply them or divide them in the near future. Here are some facts about factorials (math pun!) that you may or may not be familiar with:

(1) $n! = n(n-1)!$
(2) $\frac{n!}{(n-1)!} = n$
(3) $n! + n * n! = (n+1)!$
(4) $n^2(n-1)! + n! = (n+1)!$

You can convince yourself that these are true by plugging in numbers. In the first one, if $n = 7$, then $n - 1 = 6$, and 7!=7*6!, which is obviously true.

ex: What is the numeric value of $\frac{6!}{3!3!}$?
$\frac{6!}{3!3!} = \frac{6*5*4*3*2}{3*2*3*2} = 20$

Definition- Given any number n, the **CEILING FUNCTION of n**, $\lceil n \rceil$, is the smallest integer greater than or equal to n.

Definition- Given any number n, the **FLOOR FUNCTION of n**, $\lceil n \rceil$, is the largest integer less than or equal to n.

This isn't anything too difficult, but let's look at some examples:

ex: $\lceil \frac{3}{7} \rceil = 1$, $\lfloor \frac{3}{7} \rfloor = 0$
ex: $\lceil 8 \rceil = 8$, $\lfloor 8 \rfloor = 8$
ex: $\lceil -\sqrt{5} \rceil = -2$, $\lfloor -\sqrt{5} \rfloor = -3$

The only one that might be a bit confusing is the last one. Just keep in mind that the ceiling function "rounds up" and the floor function "rounds down". When we round a negative number up, the absolute value of that number decreases. Now let's look at a few more properties of the ceiling and floor functions.

THEOREM (1.3.1)- If $a \in \mathbb{Z}$ and $b \notin \mathbb{Z} \longrightarrow \lceil a+b \rceil = a + \lceil b \rceil$. The same applies to the floor function.
Proof- We leave the proof as an attempted exercise at the end of the section.

ex: If $n \geq 1$, solve for $\lceil \frac{n+1}{n} \rceil$.
It may appear as though the answer changes as n does, but this is not the case. $\lceil \frac{n+1}{n} \rceil = \lceil 1 + \frac{1}{n} \rceil = 1 + \lceil \frac{1}{n} \rceil \rightarrow$ Now, if $n \geq 1 \rightarrow \lceil \frac{1}{n} \rceil = 1$, so our solution is 1+1=2.

Q: Is $\lceil x+y \rceil = \lceil x \rceil + \lceil y \rceil$?
Ans: If it is, we have to prove it somehow. If it is not, it suffices to find a single example where this is untrue. Try $x, y = .1$. Then $\lceil .1 + .1 \rceil = 1$, whereas $\lceil .1 \rceil + \lceil .1 \rceil = 2$. So the two quantities are not equal.

We will be using the floor and ceiling functions when we apply something called the Pigeonhole Principle later in the semester. This requires us to solve algebraic expressions that involve these functions. In order to solve these algebraic expressions, we must fully understand what it is we are dealing with. The following questions will help with that understanding.

ex: Solve for x: $\lfloor x \rfloor = 6$

Ans: There is no algebra that will give you the answer to this one; instead we will analyze the expression and come up with a solution. Remember that $\lfloor x \rfloor$ means that we are rounding x down to the nearest integer. If the floor of x is equal to 6, it means that x was rounded down to 6. What numbers round down to 6? The solution is $6 \leq x < 7$.

Floor and ceiling functions are interesting in that they change equalities to inequalities. But just as in any algebraic equation, the ultimate goal should be to isolate the variable.

ex: Solve for x: $\lceil \frac{x}{7} \rceil = 3 \rightarrow 2 < \frac{x}{7} \leq 3 \rightarrow 14 < x \leq 21$
ex: Solve for $x: \lfloor 2x - 5 \rfloor = 12 \rightarrow 12 \leq 2x - 5 < 21 \rightarrow \frac{17}{2} \leq x < 9$

Identity and Inverse

The second half of this section deals with the concepts written above. You've no doubt heard and even worked with identites and inverses in the past, but the work we will do with it in this course is probably a step above what you've attempted before.

Definition- Given a set S under an operation *, and an arbitrary element $x \in S$, the **IDENTITY** of that set is an element $e \in S$ such that $x * e = x$.

One thing that you should know about an identity, is that it is universal for the set from which it comes. That means there is one and only one identity element per set per operation. This may be confusing, because we haven't mentioned sets or operations yet. If it helps, just remember that an operator is a mathematical object like a + sign or a multiplication sign. These examples should help.

ex: The identity of $\mathbb{R}$ under addition is 0, because given any element in the set of the Reals, adding zero gives you back the element.
ex: If you are dealing with the set of all odd integers, then the identity element under multiplication is 1, because 1 multiplied by any odd number k will give you k.

Both of those examples dealt with known sets and known identity elements. Sometimes, however, the set and operator is defined as something strange or plain unfamiliar.

ex: $S = \mathbb{R}; a, b \in S$. Define an operation as $a * b = a + b + 3$. What is the identity

element for this set under this operation?
Remember that the identity, e, fulfills the relationship $a * e = a$. So we must use the operation given in the question: $a*e = a$ But $a*e = a+e+3$, so $a+e+3 = a \rightarrow e = -3$

The idea here is to find the identity, so we simply set up the equation and solve for e. If you are given a strange set and operation, you can end up with identity elements that seem weird.

<u>*Definition*</u>- Given a set S, an element $x \in S$, and an operation *, the **INVERSE** of x is the element x^{-1} s.t. $x * x^{-1} = e$.

It is important to recognize that while there is only one identity element per set, each inverse is unique to its partner element. Not every element in a set necessarily has an inverse, and no two elements in a set will have the same inverse. Furthermore, you cannot calculate an element's inverse unless you have first found the identity element for that set.

<u>ex</u>: $S = \mathbb{R}$, and the operation is multiplication. Then the inverse of $\frac{5}{6} = \frac{6}{5}$.
<u>ex</u>: $S = \mathbb{C}$. What is the inverse of 3? This is impossible to answer, because we have not defined what the operation is. If the operation was addition, then the inverse would be -3.
<u>ex</u>: $S = \mathbb{Z}$ under multiplication. The element 7 has no inverse, because you would need to multiply 7 by $\frac{1}{7}$ to get back to 1, but that number is not an element in the set.

<u>ex</u>: $S = \mathbb{R}, a, b \in S$, where $a * b = a + b + 3$. What is the inverse element for the element 10?
So, in an earlier example we found the identity of this set to be -3. So use the definition of inverse of a to solve for 10^{-1}. $\rightarrow 10 * a = -3$. By the definition of our operator $10 * a = 10 + a + 3 = -3 \rightarrow 13 + a = -3 \rightarrow a = -16$.

<u>Exercises</u>

1. Find the numerical value of $\frac{15!}{10!5!}$
2. Find the value of $5! + 5! + 5! + 5! + 5!$
3. Prove (3) and (4) in the factorial section.
4. Prove Theorem (1.3.1).
5. Find these values:
   (a) $\lceil 1.1 \rceil$

(b) $\lfloor 1.1 \rfloor$

(c) $\lfloor -.1 \rfloor$

(d) $\lceil -2.99 \rceil$

(e) $\lfloor \frac{1}{2} + \lceil \frac{1}{2} \rceil \rfloor$

6. The function $\lceil \frac{n+1}{n} \rceil$ takes on what values if $n < 1$?

7. Is $\lfloor x - y \rfloor = \lfloor x \rfloor - \lfloor y \rfloor$? How do you know?

8. Graph the following function:

   (a) $\lfloor x \rfloor$

   (b) $\lceil 2x + 3 \rceil$

9. Prove that if x is a real number, then $\lfloor -x \rfloor = -\lceil x \rceil$.

10. Find x^{-1} in both $(\mathbb{C}, +)$ and $(\mathbb{C}, \cdot)$

   (a) -1

   (b) $\frac{1}{7}$

   (c) 0

   (d) i

   (e) $\frac{2+i}{3-i}$

What is a proof? We probably all have an intuitive understanding of the concept, but let's state it anyway. A mathematical proof is a way to show that if an assumption is true, then a resulting statement is true. If something is proven, there can be no doubt whatsoever that the statement is true. Sometimes this requires trying out a thousand (or more) cases to show that a property holds each and every time. Sometimes it requires clever and twisting arguments, using dozens of definitions and other irrefutable mathematical facts to prove a seemingly simple point. There are many proof techniques that you will learn over the course of your math career, but we will start with simple direct proofs.

(2.1) – Direct Proofs

You've encountered mathematical proofs before. Usually they were algebraic in nature- for example, you probably used the fact that $tan(x) = sin(x)/cos(x)$ to prove that $1 + tan^2(x) = sec^2(x)$. Maybe that wasn't such a difficult one- you used the definition, plugged into the equation, found a common denominator and equated both sides. Algebraic proofs can be fun because you see two completely different things on either side of an equal sign, and using simple mathematical manipulation, they end up being the same thing!

If only all math proofs were algebraic- then every high school 10th grader could be a mathematician and you wouldn't feel so special any more! So it's time to look at slightly more complex proofs- those where a statement is given....... and that's it. You have to prove it. An example of open math statements might be "The sum of two odd numbers is even", or "Every positive integer has a multiplicative inverse". Here is how we would write the second one using the mathematical language you learned in the previous chapter:

$\forall x \in \mathbb{Z}^+, \exists x^{-1} : x * x^{-1} = 1$

Do you think you could prove that (seemingly) simple fact? As budding math people, one of the things you will have to learn is whether or not something can be proven. Put in other terms, is a mathematical statement a $defintion$, or is it something that requires a proof? For the record, the above statement is a Ring *axiom*, or a given fact about the ring of integers. Don't worry about knowing what a Ring is...... that's beyond the scope of this course.

So we can't prove the inverse statement, but what about the first one? Is that first statement a given- something inherent to a set like the integers? Or is it a statement that can be proven? As you may have guessed, it is a provable statement...... but what does that even mean at this point? It may be intimidating to think that there is this statement just floating out there, and even though we *know* it to be true, we can't *be sure* that it's actually true. You know that if you add 5 and 7 you get an even number; you even know what number you get- 10477652. You probably think that this happens all the time- you add two odds and you definitely get an even. But what if you add some extremely large odd numbers, maybe a trillion digits each, and they sum to another odd integer? How could you prove that this doesn't happen? Well it turns out that you CAN prove that it doesn't happen, and we will use a direct proof to show this.

The first step in proving this statement is understanding the concept of a $definition$. So let's define the word definition in a mathematical sense: a **DEFINITION** describes a mathematical term in an unambiguous way. This definition can be a formula, a list of properties, or even just a bunch of sentences. Either way, once you have a definition, you have a way to construct a mathematical proof. Every single proof you will encounter in this course requires the use of definitions to complete. It is important to note that EVERY SINGLE TIME you see a term that has been defined, you should USE THAT DEFINITION to proceed. Let's look at the previous statement about odds and evens:

The sum of two odd numbers is even.

Here is another way we could write this, though it may seem awkward due to the simplicity of the statement:
If you have two odd numbers $\longrightarrow$ *they will sum to an even number.*

The reason we write it this way is to put it in **IF/THEN form**. A statement that is in **IF/THEN form** is one that has the assumptions on the left side and the thing we wish to prove on the right. This is useful when we wish to attempt a **DIRECT PROOF**, or a proof where we simply use the assumptions to verify the truth of a statement. Nothing fancy, which is why it is called "direct".

Now that we've decided to use a direct proof, we have to look at the assumption, which is simply that we have two odd numbers. How can we use that to prove something? We need to rigidly define the concept of odd and even. So let's get some definitions out of the way.

Definition- The **PARITY** of an integer is the property of it being either even or odd.

A few examples: The parity of -7 is odd while the parity of 204 is even.

Definition- An **EVEN** number can be written in the form $2k$, where k is an integer.
Definition- An **ODD** number can be written in the form $2k+1$, where k is an integer.

ex: 14 is an even number because $14 = 2k$, where $k = 7$.
non-ex: 15 is *not* an even number because $-19 = 2k$ results in $k = -9.5$, but -9.5 is not an integer. -19, however, IS an odd number, because $-19 = 2k + 1$, where $k = -10$.

Now we are ready to (finally) finish that proof about the odds adding to an even. Here is the proof, in its entirety:

If you have two odds $\longrightarrow$ *they add to an even*
Take two integers: x and y. By assumption they are both odd, so $x = 2k + 1$ and $y = 2l + 1$. Note that we have to use TWO DIFFERENT LETTERS, k and l. Our two odds are not the same number, so we cannot represent them with the same letter. Now, since we know what we want our result to be, we hope the result of our sum is some number of the form $2m$, which is the definition of an even number. Computing $x + y$ gives us $(2k + 1) + (2l + 1) = 2k + 2l + 2 = 2(k + l + 1)$, which, if we apply the simple substitution $k + l + 1 = m$, yields the sum we were looking for: $2m$.

■

See that black square above and to the right? That means that we have completed our proof. You'll be seeing that often in this book.

I'm sure you fully understood the work above, but just in case, I'd like to highlight the important facets of the proof. We rewrote the statement in if/then form to make it easier to see our assumption and result. We applied the relevant definitions to change our words into an equation, making sure to use different letters for different numbers. We then used simple algebra to create a compact statement that conformed to our definition of even. Done and done. Note that the substitution at the end of the proof was only written to help the student better see that we had actually achieved the definition that we were looking for. We just as easily could have ended the proof at the point where we saw $2(k+l+1)$ if we noticed that it fulfilled the definition of even.

IMPORTANT!!! Please pay attention to what you are about to read. You may be wondering why, in the previous proof, we did not just plug in two random odd integers and show that they add to an even. For example, you may have decided to say "Well, I know this: 3+5=8. Two odds add to an even. This will always happen." Maybe you are right and maybe you are wrong, but by plugging in specific values, you have proven nothing beyond the fact that those particular values possess the desired property of the proof. But bluntly, in the 3+5 example, all you would have proven was that if you add the odd number 3 and the odd number 5, you get an even number. This tells you nothing about what would happen if you added 11 and 17..... for all you know you might get an odd. So let's say this again.....

YOU CANNOT PROVE A THEOREM BY PLUGGING IN NUMBERS!!!!! DON'T DO IT!!!!!

Now that that's out of the way, let's try another.

If x is odd $\longrightarrow x^2$ is odd
If x is odd, then $x = 2k+1$. We are looking for x^2, so $x^2 = (2k+1)^2 = 4k^2+4k+1 = 2(2k^2+2k)+1$, which is, by definition, an odd number.

■

If x is even $\longrightarrow 3x+6$ is even
$x = 2k$, so $3(2k)+6 = 6k+6 = 2(3k+3)$

■

If y+7 is even, then y is odd
$y+7 = 2k \rightarrow y = 2k-7 = 2(k-3)-1$

■

These parity proofs have followed a fairly simple template- apply a definition and then manipulate terms. While definitions are vital for understanding and translating words into mathematical statements, we can also use previously proven theorems to prove new theorems. Here is an example:

If x is odd $\longrightarrow x^4+5$ is even
We know from our previous proof that if x is odd, then x^2 is odd. Well, if x^2 is odd, then the square of that number, x^4, is also odd. So $x^4 = 2k-1$. Then $x^4+5 = 2k+1+5 = 2k+6 = 2(k+3)$

Q.E.D.

A few things- That Q.E.D. also marks the end of a proof. Write it on a test to look like you know what you are doing. Also, we used $2k-1$ instead of $2k+1$ to denote an odd number. Really, we can use either one as our definition. As a matter of fact, we can use $2k+$ any odd number in our definition. Can you figure out why?

Now that you have seen a bunch of parity proofs, it is time to move on to direct proofs involving other definnitions. In that spirit......

Definition- The **ABSOLUTE VALUE** of a number $x, |x|$, is a piecewise function that is defined as x if $x \geq 0$ and $-x$ if $x < 0$

This may seem like a different definition than the one you learned in high school, as most students simply believe absolute value to mean that you change a negative to a positive. While it may be true that the absolute value changes a negative value to its positive counterpart, it says nothing for what happens if the number starts as positive. We know that the absolute value would do nothing to the number, but how do we express the duality of the function in a compact way? That is why we had to define absolute value the way we did- to account for both possibilities.

ex: $x = -3$ Well, $x < 0$, so according to the definition, $|x| = -x$. Well, $-x$ in this case is $-(-3) = 3$, which is what we would expect from an absolute value.
ex: $x = 1.6$ By our definition, $x \geq 0$, so $|x| = x = 1.6$

Now we are ready to attempt some direct proofs using this definition.

THEOREM (2.1.1)- $|xy| = |x||y|$
Proof- We know that we must use the definition of absolute value in order to complete this proof, but it might not be obvious exactly where we need to start. The problem lies in coming up with a way to express the absolute value of the product xy. Our definition relies on knowing whether the thing inside the absolute value is positive or negative, but in this case, that depends on whether x and y are positive or negative. So for this problem, we are forced to do a **PROOF BY CASES**, or a proof that exhausts every possibile scenario in an attempt to show a property holds for *every* scenario. But what are the cases that we need to examine in this proof? Well, we know that our definition relies on positivity and negativity (is that last one a word?) so we should consider every combination of positives and negatives that can appear in the product xy.
case 1: x is positive, y is positive. In this case, the product xy is a positive number, so by the definition of absolute value, $|xy| = xy$. Now look at the other side of the equation, $|x||y|$. Well, since both x and y are positive, $|x| = x$ and $|y| = y$, so $|x||y| = xy$. Since both sides of the equation are equal to xy, the two sides are equal.

case 2: x is positive, y is negative. In this case, the product xy is negative, so $|xy| = -xy$. On the right side, $|x| = x$ and $|y| = -y$, so $|xy| = (x)(-y) = -xy$. Both sides are $-xy$, so they are equal.
case 3: x is negative, y is positive. This is the same as case 2, but in reverse.
case 4: x is negative, y is negative. xy is positive, so $|xy| = xy$. $|x| = -x$ and $|y| = -y$, so $|x||y| = (-x)(-y) = xy$. Again, the two sides are equal.

Note that in ALL FOUR cases, we showed that both sides are equal to each other. These four cases comprise EVERY possible pairing of a positive and negative number, so there has been no case left out. Thus, no matter what pairing of numbers we use, $|xy| = |x||y|$

■

If you are going to attempt a proof by cases, it is important to know what cases you must attempt. In the previous theorem, we checked positives and negatives because the definition of absolute value changed based on whether the numbers were greater than or less than zero. In other proofs, your cases may be different, but be sure that the cases you choose are relevent to the statement you are trying to prove. Here is another example.

THEOREM (2.1.2)- *If the product of two numbers is even, then at least one of the two numbers must be even.*
Proof- It's probably easy to figure out that the cases here have to do with parity. If we restate the theorem as "If xy is even, then at least one of x or y is even", we easily see what the four cases are. For the sake of brevity, we will only look at three cases. It is only necessary to check the case where one of x or y is even and the other is odd.
case 1: x is even, y is even. So $x = 2k$ and $y = 2l$. $xy = (2k)(2l) = 2(2kl)$ This tells us that the product of x and y is even.
case 2: one of x and y is even, the other is odd. Without loss of generality, we will say that x is even and y is odd. Then $x = 2k$ and $y = 2l + 1$. So, $xy = (2k)(2l + 1) = 4kl + 2k = 2(2kl + k)$, which is an even number.
case 3: x is odd, y is odd. $x = 2k + 1$ and $y = 2l + 1$. $xy = (2k + 1)(2l + 1) = 4kl + 2k + 2l + 1 = 2(2kl + k + l) + 1$, which is odd.

We have tried every possible case. You can see that every single time we got an even product, one of either x or y was an even number. This proves our theorem.

■

A few more notes about this proof...... We said "without loss of generality" to signify that it didn't matter which of the two numbers was odd and which was even. The proof for either is identical, and thus we forgo the redundant work.

A question a student might ask is whether or not case 3 was even necessary. Neither of the two numbers was even, so what is the justification behind checking their product? It turns out that it was absolutely necessary that we check case 3; as a matter of fact, it was the only case we even needed to check! This may seem counterintuitive, but bear with me. Our assumption was that the product was even, and the statement is only UNTRUE when both x and y are odd. We simply need to make sure that the product of two odds does NOT give us an even, and we are done. We checked all three cases to be thorough, but it was really unnecessary.

There are a few more things to beware when attempting proofs. Students will often attempt to prove the **CONVERSE**, or reverse of the statement. It is important to realize that a statement and its converse are not the same. Proving one does not prove the other. Here is an example showing the discrepency between the two:

ex: *If x is an odd number, then $2x$ is an even number.* This is very easy to prove. Simply set $x = 2k + 1$, double it and show that the result is even. But let's look at the converse of the statement, namely "If $2x$ is an even number, then x is odd". We would start by using the definition of even, and claiming that $2x = 2k$. After dividing both sides by 2, we get $x = k$. What does this tell us about x? Absolutely nothing, as k is not inherently odd or even. For example, if $2x = 6$, we end up with $6 = 2k$, and $k = 3$. So the converse of a true statement is not necessarily true, and attempting to "prove it in reverse" often results in incorrect math.

Now, there are many other proof methods that we will discuss in future chapters, including proof by contrapositive, proof by induction, combinatorial proofs, etc. They require a bit more thought, and often cleverer "tricks" than we have displayed up to this point. Even so, a direct proof is often more than enough to tackle some difficult theorems. Unless you are certain of how to proceed, you should attempt a direct proof before using any other method.

EXERCISES

1. What is the parity of the number 47? -500? $\sqrt{12}$?

2. Prove: The sum of an odd number and an even number is odd.

3. Prove: The product of three odd numbers is odd.

4. Use the proof in the previous question to show that the product of six odd numbers is odd.

5. Prove that if x is odd, then $3x + 11$ is even.

6. Give a proof by cases to show that if the product of two numbers is odd, then both numbers are odd.

7. Suppose $x^3 + 2xy^2 \geq 2x^2y + 4y^3$. Show that $x \geq 2y$

8. If $x(y - 1)$ is even, show that x is even or y is odd.

9. How many cases were required to prove the statement in the previous question? How do you know?

10. How many cases would it take to prove that $|xyz| = |x||y||z|$? What are those cases?

11. Define a **RATIONAL NUMBER** as any number that can be expressed as p/q, where p and q are both integers, and $q \neq 0$. Define an **IRRATIONAL NUMBER** as a number that is not rational.

    (a) Prove that the sum of two rational numbers is rational.

    (b) Is the converse of the previous statement true or false? If it is true, prove it. If it is false, find a counterexample that disproves it.

    (c) Prove that if x is rational, then $1/x$ is rational.

12. Use a direct proof to show that the sum of an odd number of odd numbers is odd. Use only the definition of odd, and no previous proofs.

13. Here is a good test to see if you understand which cases are important: You are given a deck of cards that are two sided- on one side is a letter and on the opposite side is an integer. You are told that every time you see a vowel, there is an even number on the other side, but you are skeptical and want to see if this is true. There are four cards on a table- an ”A”, a ”3”, a ”10” and a ”T”. Which cards MUST you turn over in order to determine whether or not the deck is as you were told it was? Your goal should be to turn over the MINIMUM number of cards to determine the truth of the statement.

14. Prove: If $x > y \longrightarrow |y - x| = x - y$

(2.2) – More Proofs

Last chapter, we worked on proofs that could be tackled directly. Of course, it will not always be the case that we can use the assumptions to prove the result. For statements that cannot be proven in this manner, we will attempt to use an **INDIRECT PROOF**, or a **PROOF BY CONTRAPOSITIVE**. Before we discuss exactly what this process entails, we will motivate via an example, and give a brief justification for why it works.

ex: *If* $3x - 8$ *is odd, then* x *is odd*
We can try to prove this directly, but let's see where that takes us. If $3x - 8$ is odd, then $3x - 8 = 2k + 1$. Then $3x = 2k + 9$. $x = \frac{2k}{3} + 3$. An immediate problem arises- we don't know if x is even an integer, let alone an odd integer. So our direct proof fails, and we need to figure out a different way to prove this statement.

To that end, we are going to apply a bit of logic. We stated in 2.1 that the converse of a statement is not the same as the original. We now introduce the concept of the *contrapositive* of a statement, and will use it to complete our previous example.

Definition- The **CONTRAPOSITIVE** of the statement $p \longrightarrow q$ is the statement $\sim q \longrightarrow \sim p$

The reason why the contrapositive of a statement is so important is because it has the SAME TRUTH VALUE as the original statement. This means that if we can prove the contrapositive of a mathematical statement, we have also proven the original statement. The first thing we should do with this information is figure out how to correspond these if/then statements to p's and q's.

Look at the statement "If x is odd, then x^2 is odd". In this case, the p is "x is odd" and the q is "x^2 is odd". The contrapositive of that statement is "If x^2 is NOT odd, then x is even". We can replace "NOT odd" with even. So simply put- the contrapositive of an if/then statement reverses and negates the terms. Now back to our original example.

ex: (again)- *If* $3x - 8$ *is odd, then* x *is odd*
We know that a direct proof is impossible, so we attempt a proof by contraposition. The contrapositive of the statement is "If x is even, then $3x - 8$ is even". This is much easier to prove! $x = 2k$, so $3(2k) - 8 = 6k - 8 = 2(3k - 4)$, which is even.

Q.E.D.

And now we have another way to prove a statement. But it should be noted that once the contrapositive is applied, you will proceed as though you are attempting a direct proof. Use the assumptions to prove the conclusion. Throughout this course, you will mostly use contraposition when the resulting statement is less complicated than the assumption.

ex: x *is odd* $\longleftrightarrow 9x + 14$ *is odd*
That double arrow is new, but it really isn't that difficult to deal with. It signifies an **IF AND ONLY IF PROOF**, which is a proof that must completed both forwards and backwards. To put it in math parlance, we will prove both the statement and its converse. Since an if and only if proof is really two proofs in one, we will treat it as such.
$\Longrightarrow$ (means from left to right) x is odd, so $x = 2k - 1 \rightarrow 9(2k - 1) + 14 = 18k + 5 = 2(9k + 2) + 1$ Done.
$\Longleftarrow$ Remember that we are attempting to prove the converse here, or "If $9x+14$ is odd, then x is odd. Since the assumption is more complicated than the result, we will use contrapositive, or "If x is even, then $9x+14$ is even". $x = 2k \rightarrow 9(2k)+14 = 2(9k+7)$

So, we have proven both the original statement and its converse. This concludes the if and only if proof.

Q.E.D.

ex: $x^3 + 2x - 10$ *is odd* $\longrightarrow 7x - 4$ *is odd*
This one is a mess, but I think most would agree that the result is less complicated than the assumption. So we start by applying contrapositive, and coming up with the statement "If $7x - 4$ is even, then $x^3 + 2x - 10$ is even". Maybe this doesn't seem any easier, but we can do it. If $7x - 4$ is even, then $7x - 4 = 2k$. Let's proceed in a slightly different manner this time. If we were to add 4 to both sides, we would end up with $7x$ =an even number. This implies that x is an even number, because if x were odd, $7x$ would be odd. So we know now that x is even. From this point it's easy. $x = 2l \rightarrow x^3 + 2x - 10 = (2l)^3 + 2(2l) - 10 = 8l^3 + 4l - 10 = 2(4l^3 + 2l - 5)$, which is even. Since the contrapositive of the original statement is true, so is the original statement.

■

In the previous example, we took the intermediate step of showing that x had to be even. So it turns out that we had three statements in this proof that were all **EQUIVALENT**. This means that any of the truth of any of the three statements implied the truth of the other two. We can often prove a "chain" of arbitrarily many statements in the same way. We will call these types of proofs **EQUIVALENCE PROOFS**. In an equivalence proof, we must create a loop that connects the first statement to the second, the second to the third, and so on until the final statement connects back to the first. Here is an example of an equivalence proof:

(1) $x > y$
(2) $|y - x| = x - y$
(3) $|x - y| = x - y$
Now we will illustrate how to complete this equivalence proof. We want to complete the following three proofs: (1) → (2), (2) → (3), and (3) → (1). This will complete a loop that chains all of the statements together. We could have proven (1) → (3), (3) → (2), and (2) → (1), but either way is fine.

(1) $\implies$ (2): $x > y \to y - x < 0 \to |y - x| = -(y - x) = x - y$
(2) $\implies$ (3): $|y - x| = x - y$ implies that $x > y$. So, $|x - y| = x - y$
(3) $\implies$ (1): $|x - y| = x - y \to x > y$ by definition of absolute value.

$\blacksquare$

ex: $\forall x \in \mathbb{Z}, 1 \leq x < 6 \longrightarrow x^3 \geq x!$
This one is fairly obvious, and also very easy to prove. The example is asking us to show a certain property for a finite number of specific x's. Thus, we will apply a **PROOF BY EXHAUSTION**, which is the process of trying every single number in the given set to show that the property holds for each. For this question, we need only to check that the statment is true for $x = 1, 2, 3, 4, 5$. Essentially, we will "exhaust" every single possitbility and show the statement to be true each time. When $x = 1, x^3 = 1$ and $x! = 1$. When $x = 2, x^3 = 8$ and $x! = 2$. For $x = 3, x^3 = 27$ while $x! = 6$. When $x = 4 \to x^3 = 64, x! = 24$. Finally, for $x = 5 \to x^3 = 125$ and $x! = 120$. Our proof is done; we have shown the statement to be true for each number in the given set.

Q.E.D.

Note that there is very little difference between a proof by cases and a proof by exhaustion. Basically, if the cases are specific numbers instead of general sets of numbers, we will refer to our process as a proof by exhaustion. Now, what if we were to make a slight modification to the previous question, asking instead......

ex: $\forall x \in \mathbb{Z}, 1 \leq x < 6 \longrightarrow x^3 > x!$
Can we prove this statement in the same way? The answer is NO- we cannot prove it at all. The statement is not true for all elements in the given set. When $x = 1$, both x^3 and $x!$ are equal to 1. Thus, we have proven the statement untrue by simply stating a *counterexample*. We call this process **DISPROVING BY COUNTEREXAMPLE** because we are finding a single instance within the set for which the conclusion

is proven false. Note that we do not need to show that the statement is untrue for all values in the set- we need only show it is untrue for one. In our example, the number 1 was our counterexample.

It is an important skill to be able to pick out the single (or multiple) counterexample that disproves a rule. Back in Chapter 1, you were asked to determine the truth value of several quantifier statements. If you found the statement to be untrue, you were asked to find a counterexample. When attempting to prove a mathematical statement, you will not always know whether a conclusion is true or false. Determining which numbers will ”mess it up” is a vital step in gaining an understanding of advanced concepts. Look at the following statements and try to find a counterexample to disprove each. The answers will be immediately below, but try not to cheat.

1. $\forall x \in \mathbb{Z}, x^4 > 0$
   This is true...... most of the time. But that pesky number 0 can cause problems quite often. 0^4 is not greater than zero.

2. *When $x \neq 0, x^5$ is always greater than x^2*
   So we took care of the zero, but this is not a true statement for all x. When $x = 1/2$, (or any number between zero and one, for that matter) $x^2 > x^5$.

3. *The product of the factors of x is always greater than the sum of the factors of x.*
   This is true more often than not, but if x is a prime number, the product will be less than the sum.

4. *The sum of the distances from the points A to B and B to C is greater than the distance between A and C*
   Again, it only takes one counterexample to topple a wannabe proof. If A,B and C are points in a straight line, then the sum of the distances of A to B and B to C is equal to the distance from A to C.

So one of the pitfalls in proving these various statements is that you may be attempting to prove something that is not actually true. It is important to understand exactly what it is you are trying to prove, and thus you can ensure that no counterexamples will torpedo the entire venture. Another issue that students can encounter in proof writing is a misapplication or misunderstanding of the fundamental rules of algebra or arithmetic. Look at the following, seemingly correct proof, and try to determine where the mistake lies. We begin by giving you the piece of information $a = b$, and perform basic algebraic steps to come to the clearly absurd conclusion that 1=2.

$a = b$ Given
$ab = b^2$ Multiply both sides by b
$ab - a^2 = b^2 - a^2$ Subtract a^2 from both sides
$a(b - a) = (b + a)(b - a)$ Factor
$a = b + a$ Divide by $b - a$
$a = 2a$ Replace b with a
$1 = 2$ Divide by a

Have you figured out where the mistake is? As stated earlier, the problem lies with a (hidden) algebraic mistake. The proof goes wrong when we attempt to divide $b - a$ on both sides. Because $b = a, b - a = 0$. It is a well-known fact that you cannot divide by 0. Maybe this gives you a bit more insight as to why that is. When you divide by 0, you can prove *anything* is equal to anything else. What lesson should you take from this? Be careful and make sure you are following all the proper rules of algebra and arithmetic.

We will end this section with one final proof technique- the **PROOF BY CONTRADICTION**. You probably used this technique in geometry proofs in high school, and here it is no different. The idea is to assume the OPPPOSITE of the conclusion of the statement that is given. We will then attempt a direct proof using this opposite assumption. If, during the course of our proof, we reach some sort of contradiction, we know that the mistake was with our assumption. Since the assumption was the opposite of what we were trying to prove, the original conclusion must be correct. Now maybe that sounded like gibberish, so let's put it into action with two very different proofs.

ex: *If there are fifteen people in the same room together, at least three of them were born on the same day of the week.*
Because we are attempting a proof by contradiction, we will assume the opposite of our result. That means that no more than two will share a same-day birthday. Since there are seven days of the week and at most two were born on the same day, there can be no more than 14 people in the room- two for each day of the week. But that contradicts the fact that there are 15 people in the room. So our assumption must be incorrect, and we now know that at least three were born on the same day of the week.

THEOREM (5.2.1)- $\sqrt{2}$ *is irrational*
Proof- This one is much more difficult. Let's review the definition of a rational number as given in the previous chapter: A *rational* number is a number that can be written as p/q, where p and q are integers and $q \neq 0$. But we are assuming the opposite of our conclusion, so we will say that $\sqrt{2}$ is rational. So........

$\sqrt{2} = \frac{p}{q}$ Definition of a rational number
$q\sqrt{2} = p$ Cross multiply
$2q^2 = p^2$ Square both sides
p is an even number Definition of an even number
$2q^2 = (2k)^2$ Replace p with $2k$
$2q^2 = 4k^2$ Expand the right side
$q^2 = 2k^2$ Divide by 2
q is an even number Definition of an even number
$(2l)^2 = 2k^2$ Replace q with $2l$

We are going to stop here and point out something you may not yet realize. The next steps would be to expand and then divide both sides by 2. We could then claim k was an even number and replace it with $2m$. Have you figured out why this is problematic? Think about it for a moment. We could repeat this process INDEFINITELY. Over and over and over again ad infinitum we could keep expanding, dividing by 2, claiming that our new variable is even. The process would literally never end, and in math this contradicts something called the **WELL ORDERING PRINCIPLE**, or the idea that the set of integers has a smallest element. Every time we divide by 2, we are cutting our integers in half, and we could do this an infinite number of times. Eventually we would divide so many times that our number would necessarily decrease below 1, which is impossible for a positive integer. So we have found our CONTRADICTION, which means that our assumption was untrue. Therefore, $\sqrt{2}$ is irrational.

■

proof checklist

(1) *Direct Proof*- Use the assumptions to prove the conclusion
(2) *Proof by Cases*- We can sometimes place number in sets that all possess a particular property. By testing every combination of these sets, we can determine a universal property
(3) *Proof by Contraposition*- If the conclusion is more complicated than the assumptions, we prove the "opposite"
(4) *If and only If Proof*- We must prove the original statement and its converse
(5) *Equivalence*- Create a chain between multiple statements with the added provision that the final statement implies the first
(6) *Proof by Exhaustion*- Modified proof by cases where we attempt every single number in a set to determine a universal property
(7) *Proof by Contradiction*- Assume the opposite of the result and establish a contradiction

These are not the only techniques you will learn, but they will be sufficient for 80 percent of the proofs you will attempt in this course. The sheer number of possibilities may seem intimidating at first, but this list should help you get started. For now, just keep track of consistencies between the various proofs, and attempt to form a plan of attack for each. Look for familiar signs within the context of the questions that will give a hint as to which way to go. As you do more and more examples and start to prove more difficult theorems, determining which proof method to use will become easier.

Exercises

1. Prove that if $x^2 + 4x - 9$ is even, then x is even.
2. Prove that n is even if and only if $9n - 2$ is even.
3. Prove that $m^2 = n^2$ if and only if $m = n$ or $m = -n$.
4. Prove or disprove via counterexample: The product of any five consecutive numbers is divisible by 8.
5. Prove or disprove via counterexample: The sum of two irrational numbers is irrational.
6. Prove that the following statements are equivalent:
   (a) $3x + 2$ is even
   (b) $x + 5$ is odd
   (c) x^2 is even
7. Show that at least three of any 25 days must fall in the same month of the year.
8. You have a bag containing blue and red marbles. If you choose five marbles from the bag at random, prove that you have chosen two pairs of marbles of the same color.
9. Prove that the following statements are equivalent:
   (a) $a < b$
   (b) The average of a and b is greater than a
   (c) The average of a and b is less than b
10. Prove: $3x^2 + 10x - 2$ is odd $\longleftrightarrow 7x^3 + 13x$ is even.

(2.3) – Mathematical Induction

Look at the following question:

What is the sum of the first n consecutive positive odd numbers?

How would a student go about trying to figure this one out? When we ask for the first n odd positive odd numbers, what exactly do we mean? Since n can be any number, we would expect our answer to be some sort of formula in terms of n. But how can we go about deriving a formula of this nature? Remember the first rule of doing proofs- plug in numbers and see what happens! Let's do that for this question. Now take a close look at what n represents- it tells us the number of consecutive positive odds (starting with the number 1) we will be adding. For example, if $n = 6$, we will be adding 1+3+5+7+9+11, because those are the first 6 odd numbers. Note that n isn't necessarily an odd number; it is simply tells us how many odds we need to add.

Once we understand what n represents, we can start plugging in numbers for n to see if we can figure out some kind of pattern. If we find a pattern, we may be able to develop a formula that answers our original question.

$n = 1 \Longrightarrow$ Sum=1
$n = 2 \Longrightarrow$ 1+3=4
$n = 3 \Longrightarrow$ 1+3+5=9
$n = 4 \Longrightarrow$ 1+3+5+7=16
$n = 5 \Longrightarrow$ 1+3+5+7+9=25

That's probably more than enough. By now, you've surely noticed the pattern that is developing. The sum of the first n consecutive positive odd numbers is always equal to n^2. We said "always" in the previous sentence, but can we be sure.......? Well, if you were to try $n = 6$, you'd quickly see that the sum is 36. So our theory seems to hold, but have we actually proven anything? Remember, plugging in values for n and computing answers tells us nothing except that our property holds for that particular value for n.

So we've come up with a formula, but how to prove it? This is where the *Principle of Mathematical Induction* comes in. We will use it whenever we are attempting to verify that a formula holds for ALL INTEGERS greater than or equal to n. Before explaining the process in full, we will give an intuitive understanding of why it works. Then we will translate these words into a rigid mathematical structure that you will be able to use to prove theorems or formulas of this nature.

Try to picture this scenario, if you will. There is a ladder in front of you, and it stretches up so high that you cannot see the top rung. We will say that this ladder has an infinite number of rungs, starting with the first rung that is right in front of you. You can see that the rungs are spaced evenly apart, and if you can reach one rung, you can use that run to reach the run directly above it. For example, if you were standing on the 11th rung, you could use it to get to the 12th rung. Furthermore, you can reach the first rung of the ladder with ease. So here is the question: Based on the information you have about the ladder, to what rung could you possibly climb? Now you might want to say, ”I can only climb ’til I get tired”, or ”I can climb until I die of old age”, but you are only saying that because you are too clever for this book. Let’s assume infinited time and energy. What rung could you make it to?

The answer is- ANY rung you want. There are no obstacles in the way of your reaching the millionth, or even the billionth rung if that was your desire. You can reach the first rung, so you can begin climbing at any time. If you can reach the first rung, you know you can reach the second. If you can reach the second, you know you can reach the third. In this way, once you reach the n^{th} rung, you can use it to reach the $n{+}1^{th}$ rung. You could climb an infinite number of rungs on this ladder!

This is the gist of the principle of mathematical induction: If we can prove our formula or theorem true for an initial case (this would be the first rung of the ladder), then we have a basis from which to begin. Next, we wish to show that IF it works for the n^{th} case, then it will also work for the $n + 1^{th}$ case. By showing these two steps hold, we have proven our theorem for ALL integers greater than or equal to n.

PRINCIPLE OF MATHEMATICAL INDUCTION- To prove a propositional function P(n) is true for all positive integers n, we complete the following two steps:
(1) **basic step**- Verify that P(1) is true
(2) **inductive step**- Verify the statement $P(k) \rightarrow P(k+1)$ is true for all k

Now that we have a rigid definition out of the way, we will show how this applies to the problems you will face in this course. Let’s finish off the previous example:

THEOREM (2.3.1)- $n^2 = \sum_{i=1}^{n}(2i-1)$ Or.....
THEOREM- *The sum of the first n positive odd integers is equal to* n^2 Or.....
THEOREM- $1+3+5+7+........+(2n-1)=n^2$

Hope you realize they are all the same thing, but regardless, we will be using the latter due to its algebraic simplicity.

proof: We first complete the basic step; in this case, plugging in the number 1.

$$1 = 1 \tag{1}$$

Now, that may have seemed anticlimactic, but let me explain. When $n = 1$, all we are doing is adding the first ONE positive odds. But what is the first positive odd? 1, and so the sum is simply 1! Moving onto the inductive step.....

We want to show that if this works for k, then it works for $k+1$, so we will assume this formula true for $n = k$. This entails simply plugging in k wherever you saw an n. This step is called the **INDUCTIVE HYPOTHESIS**, and will we use it in a moment.

$$1+3+5+7+.....+(2k-1)=k^2 \tag{2}$$

Now remember, we are assuming this to be true in order to prove that the formula is true for $k+1$. So, we need to plug $k+1$ into our equation wherever we see k, and hopefully come to the conclusion that it "works".

$$1+3+5+7+......(2(k+1)-1)=(k+1)^2 \tag{3}$$

$$1+3+5+7+.....(2k-1)+(2k+1)=k^2+2k+1 \tag{4}$$

Note that for equation (4), we left in the (2k-1) term. It is important that you understand where this term is coming from. Remember that we are listing ALL consecutive odd numbers from 1 to $2k+1$ at this point, and what is the odd number directly preceding $2k+1$? It is the integer that is two less than $2k+1$, because odd numbers always differ by two. Two less than $2k+1$ is $2k-1$, and the fact that we have it written there will play an important role int he next step.

$$[1+3+5+7+.....+(2k-1)]+(2k+1)=k^2+2k+1 \tag{5}$$

Now there is a reason we placed those particular terms in brackets. Do those terms look familiar to you? If not, glance up at equation (2), which is our inductive hypothesis. They are one and the same! Because (2) is an equality, we can replace everything within the brackets like so:

$$k^2 + (2k + 1) = k^2 + 2k + 1 \tag{6}$$

Just drop the parenthasis on the left side and the equality is complete!

$\blacksquare$

A few final notes: Although 1 was the number we plugged into the basis step, this is not always the case. For example, in a proof that involved only even integers, the "first" number we would use is 2. The basis case number will be denoted in the question, so make sure you follow instructions when plugging in. Also note that we needed to use the inductive hypothesis to show that the property holds for $k+1$. If you do not use the assumption, you are not doing the proof correctly. Often the assumption will end up replacing a nice portion of the $k + 1$ equation, facilitating the equality. And finally, don't think that replacing n with k is a superfluous step- remember that n represents the n^{th} odd number, not some arbitrary rung on the ladder of odd integers.

Now that we've completed an induction proof, let's quickly recap (without all the math jargon) the steps that we took to get there.

(1) Plug the value of the initial condition into the equation. In our previous example, 1 was our first value. Make sure the two sides are the same.
(2) Replace n with k. This is our inductive hypothesis.
(3) Replace every k with $k + 1$. Use the inductive hypothesis to prove this equation true.

ex: Prove by Induction for $n \in \mathbb{Z}^+ : \frac{1}{2^1} + \frac{1}{2^2} + \frac{1}{2^3} + ... + \frac{1}{2^n} = 1 - \frac{1}{2^n}$

First we plug in 1 for our basis step, giving us $\frac{1}{2^1} = \frac{1}{2} = 1 - \frac{1}{2^1}$ Now that we have shown the basis step holds, we will replace n in the original equation with k. $\frac{1}{2^1} + \frac{1}{2^2} + \frac{1}{2^3} + ... + \frac{1}{2^k} = 1 - \frac{1}{2^k}$ is our inductive hypothesis. We then replace each k with $k+1$, yielding $\frac{1}{2^1} + \frac{1}{2^2} + \frac{1}{2^3} + ... + \frac{1}{2^k} + \frac{1}{2^{k+1}} = 1 - \frac{1}{2^{k+1}}$. But note that all of the terms from $\frac{1}{2^1}$ to $\frac{1}{2^k}$ can be replaced with $1 - \frac{1}{2^k}$ by virtue of the inductive hypothesis. Our new equation is $1 - \frac{1}{2^k} + \frac{1}{2^{k+1}} = 1 - \frac{1}{2^{k+1}}$ Let's get rid of the 1s on each side, and then get a common denominator on the left side. We now have $-\frac{2}{2^{k+1}} + \frac{1}{2^{k+1}} = -\frac{1}{2^{k+1}}$, and adding on the left side gives $-\frac{1}{2^{k+1}} = -\frac{1}{2^{k+1}}$. Our proof is done.

Q.E.D.

Now you've seen two proofs, and in each, the inductive hypothesis replaced a big portion of the $k+1$ equation. Here is an example where that does not occur.

ex: For $n \geq 1 : n! \leq n^n$

Plugging in 1, we see that $1! = 1 = 1^1$, so our basis step is done. The inductive hypothesis is $k! \leq k^k$. Replacing with $k+1$ gives $(k+1)! \leq (k+1)^{k+1}$. Now, we need to use the assumption to prove this statement, but it might not be immediately obvious how we can do this. Our goal is to create a chain of inequalities starting with $(k+1)!$ and ending with $(k+1)^{k+1}$ such that each term is less than or equal to the term immediately to its left. Our explanation will come afterward, but here is how it will look:

$(k+1)! = (k+1)k! \leq (k+1)(k+1)^k \leq (k+1)^{k+1}$

The proof is actually done, but perhaps we should explain why that middle step is a valid inequality:

$(k+1)k! \leq (k+1)(k+1)^k$, but why? Well, look at this chain: $k!$ is less than or equal to k^k based on our inductive hypothesis, and k^k is certainly less than or equal to $(k+1)^k$. This gives us $(k+1)k! \leq (k+1)k^k \leq (k+1)(k+1)^k$.

The other inequalities involve simple algebraic manipulation, nothing more.

■

Induction can be used for almost any proof where we are trying to prove something for all integers. There is another form of induction called **STRONG INDUCTION** that is done a bit differently, but the spirit is the same. For the sake of this course, we will not need to use strong induction. In future chapters, we will apply the principle of mathematical induction to prove certain universal properties about the division of equations. But for now you can take it easy, and work on mastering these basic induction questions.

Exercises

1. (a) Attempt to find a formula for the sum of the first n positive integers.

   (b) Prove your formula by induction.

2. Try to figure out a way to prove $n! \leq n^n$ without using induction.

3. Prove for $n \geq 0$: $1 + 2 + 2^2 + 2^3 + ...2^n = 2^{n+1} - 1$

4. Prove that $1^2 + 2^2 + 3^2 + ... + n^2 = n(n+1)(2n+1)/6$ for $n \geq 1$.

5. Prove that $1^2 + 3^2 + 5^2 + ... + (2n+1)^2 = (n+1)(2n+1)(2n+3)/3$ when n is a nonnegative integer.

6. For all positive n, show that $1(1!) + 2(2!) + 3(3!) + ... + n(n!) = (n+1)! - 1$.

7. Prove that $3 + 3(5) + 3(5^2) + 3(5^3) + ... 3(5^n) = 3(5^{n+1} - 1)/4$ whenever n is a positive integer.

8. Prove that $1^2 - 2^2 + 3^2 - .... + (-1)^{n-1}n^2 = (-1)^{n-1}n(n+1)/2$ whenever n is a positive integer.

9. Show that $1^3 + 2^3 + ... + n^3 = (1 + 2 + 3 + ... + n)^2$ for $n \geq 1$.

10. Prove by induction for $n > 1$: $n! < n^n$.

11. Prove that $3^n < n!$ if n is greater than 6.

12. Prove that $2^n > n^2$ if n is an integer greater than 4.

We have used the word "set" a few times before this point, but only in the loosest, most intuitive sense. Now it's time to define exactly what a set is, mention some properties we impose upon sets, and proove theorems that will help us later. We will also introduce the idea of an *inclusion proof*, which pertains to sets that are a part of larger sets. Set theory is one of the more ubiquitous branches of math- and for those of you who eschewed SAT studying, that means that you will see sets in almost every math class you take from here on out.

(3.1) – Sets

Definition-A **SET** is a collection of objects.

Definition-An **OBJECT** is something contained within a set.

That's it. That's what a set is and what an object is. If the definitions seem circular, that's because they are. The objects in a set can be anything- students in a classroom, teams that won a World Series, numbers. We will (mainly) be dealing with sets of numbers, or sets that contain other sets.

ex: $\mathbb{Z}^+ = \{1, 2, 3, 4, 5.....\}$ ex: $\mathbb{Q} = \{1, 2, \frac{1}{2}, \frac{1}{3}, \frac{2}{3}, 3.....\}$

Definition- Two sets are **EQUAL** if they contain the same elements.

ex: $\{1, 2, 3\} = \{\frac{2}{2}, \frac{4}{2}, \frac{6}{2}\}$

In simple, finite examples like the one above, it isn't so difficult to determine whether or not two sets are equal. Sometimes, however, it's not so obvious if two sets have the same elements. Here is one such case:

ex: $\{\forall x \in \mathbb{Z} : \sqrt{x} = x\} = \{0, 1\}$

Maybe that one wasn't so difficult, but you can probably tell that the examples are getting more complicated. Future examples will blur the line further, and so we will need another way to prove that two sets are equal. We will revisit that idea a little bit later, and for now define some terms and establish relationships between sets.

Definition- Set A is a **SUBSET** of set B ($A \subseteq B$) if and only if every element of A is an element of B.

The notation for a subset looks very similar to a ”less than or equal” sign, and it should be apparent why. If A is a subset of B, it has either fewer or the same number of elements as B. How do we formally show that $A \subseteq B$?

$\forall x \in A \longrightarrow x \in B$

And how to show that A is not a subset of B?

$A \nsubseteq B \longleftrightarrow \exists x \in A : x \notin B$

Try to determine in each of the following whether or not the set on the left is a subset of the set on the right. If you look below before trying them on your own, then you are a cheater!

1. $\mathbb{R} \subset \mathbb{C}$
2. $\mathbb{R} \in \mathbb{C}$
3. $\{x : x = 2k + 1, k \in \mathbb{Z}\} \subseteq \mathbb{Z}^+$
4. $\{x : x^2 < 50\} \subseteq \mathbb{R}^+$

The first thing to do is to translate each of these statements into ”english”. Only by reading these in a language we understand can we hope to make sense of them.

1. *The set of all real numbers is a subset of the complex numbers.* This is a TRUE statement, because complex numbers are of form $a + bi$, where a and b are real numbers. The set of real numbers is simply the subset of the complex numbers where $b = 0$.

2. *The set of real numbers is an element in the set of complex numbers.* Now is a good time to highlight the difference between $\subset$ and $\in$. We know that a subset is a collection of elements that is wholly contained within another set, while an element is an object in a set. A subset is not an element in a set A unless we are discussing the set of all subsets of A. If that concept is confusing, ignore it for now and simply note that while $\mathbb{R} \subset \mathbb{C}$, $\mathbb{R} \notin \mathbb{C}$

3. *The set of all odd integers is a subset of the set of positive integers.* This is obviously FALSE, as -15 is not a positive integer. The challenge here comes from translating the statement. Once that is done, the question is easy.

4. *The set of all x values that, when squared, are less than 50 is a subset of the positive integers.* This is FALSE as well. $(-5)^2 = 25 < 50$, but -5 is not a positive integer. At least I don't think it is. Again, translating the original statement into english is half the challenge.

Perhaps we should mention that there is a slight difference between $\subset$ and $\subseteq$. Just like in any inequality, the former denotes a strict "smaller than" relationship between two sets, and defines what we call a *proper subset.* The latter is simply an indication that the "smaller" of the two sets may, in fact, be the larger set.

Here is an official definition for the above term:

Definition- If A is a **PROPER SUBSET** of B, then $\exists x \in B$ s.t. $x \notin A$

★ Now would also be a good time to mention that "other" way we can determine if two sets are equal. If $A = B \longrightarrow A \subseteq B$ and $B \subseteq A$. We will be using this technique in many inclusion proofs in the next chapter.

ex: $A = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}, B = \{x : x \text{ is a subset of } \{a, b\}\}$

You may know where we are going with this one, but since $A \subseteq B$ and $B \subseteq A$, $A = B$.

I hope you didn't get too confused when you saw that $\emptyset$ symbol up there. While it pretty much IS what it looks like, a formal definition is in order.

Definition-The **EMPTY SET**, $\emptyset$, is the set containing no elements.

Note that the empty set is a subset in the previous example. As a matter of convention, the empty set is a subset of every set. Though it plays a similar role to the number 0 in other branches of math, do not confuse $\emptyset$ with $\{0\}$. The former is a set containing nothing, while the latter is a set comprised only of the number 0.

Before we get into inclusion proofs, there are few more terms that you must become familiar with.

Defintion- Let S be a set. If S contains exactly n elements, then we say S is a **FINITE SET**, and n is the **CARDINALITY** of S.

Simply put, a finite set contains a finite number of elements. The integers, for example, are not a finite set, since there are an infinite number of integers. The cardinality of a set is the number of elements in that set, and the shorthand way of noting cardinality of a set S is $|S|$. The set $\{a, b, c\}$ has a cardinality of three, while the set $\{2, 4, 6, ..., 98, 100\}$ has a cardinality of 50. Again, as a matter of convention, we say that the empty set has a cardinality of 0.

<u>Definition</u>- The **POWER SET of S**, denoted by $\mathcal{P}(S)$, is the set of all subsets of S.

<u>ex</u>: $S = \{1, 2, 3\} \rightarrow \mathcal{P}(S) = \Big\{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, S\Big\}$

Now, to be perfectly clear, although 1 is an element in set S, $\{1\}$ is a subset of S and thus contained within $\mathcal{P}(S)$. Note again how the empty set makes an appearance as an element in $\mathcal{P}(S)$. $\emptyset$ is an element in $\mathcal{P}(A)$ for all sets A.

A fair question to ask at this point is, given a set S with cardinality n, what is the cardinality of $\mathcal{P}(S)$? In our most recent example, we saw that when S contained 3 elements, $|S| = 8$. If you return to our example (on the previous page) where we listed the subsets of $S = \{a, b\}$, you'll note that $|S| = 4$. What if we were to look for the cardinality of the set $\{Mets\}$? The only subsets are $\emptyset$ and $\{Mets\}$, and thus the cardinality is 2. Perhaps you are starting to see a pattern develop?

<u>THEOREM</u>- If $|S| = n$, then $|\mathcal{P}(S)| = 2^n$.
<u>Proof</u>- We will prove this by Induction. For the basis step, we will simply note that if n=0, then $\mathcal{P}(S)$ contains only $2^0 = 1$ element, which is $\emptyset$. Next we will assume that if $|S| = k \rightarrow \mathcal{P}(S) = 2^k$. We want to show that this holds for $k+1$, and this is where it gets a little tricky. So let's say that we have a set with k elements; without loss of generality we will call those elements $\{1, 2, 3, ..., k-1, k\}$. Now we are going to add a single element to that set, and we will call it $k+1$. We know from our inductive hypothesis that our set with k elements has 2^k subsets. In each of those 2^k subsets, we can choose to either add the element $k+1$ or leave it alone. So each of the 2^k subsets spawns two separate subsets when $k+1$ is introduced. The inductive hypothesis ensures that there is no overlap between sets and that every possible subset is accounted for. This means that a set with $k+1$ elements has $2 * 2^k = 2^{k+1}$ subsets. So, given the following: $|S| = k \rightarrow |\mathcal{P}(S)| = 2^k$, we know that $|S| = k+1 \rightarrow |\mathcal{P}(S)| = 2^{k+1}$.

Q.E.D.

You just knew induction would come in handy eventually! At any rate, the most important thing you should take out of this chapter is that math has a LOT of definitions that require memorization. As you attempt the exercises, attempt to internalize all of these definitions to save yourself trouble later.

Exercises

1. List the members of these sets:

   (a) $(x : x$ is a real number such that $x^2 = 1)$

   (b) $(x : x$ is a positive integer less than $10)$

   (c) $(x : x$ is the square of an integer and $x < 100)$

   (d) $(x : x$ is an integer such that $x^2 = 2)$

2. Suppose that A=$\{2, 4, 6\}, B = \{2, 6\}, C = \{4, 6\}$, and $D = \{4, 6, 8\}$. Determine which of these sets are subsets of which other of these sets.

3. Use a Venn Diagram to illustrate the relationship:

   (a) $A \subseteq B$ and $B \subseteq C$

   (b) $A \subset B$ and $B \subset C$

   (c) $A \subset B$ and $A \subset C$

   (d) $A \subset B$ and $C \subset B$

4. Suppose that A,B, and C are sets such that $A \subseteq B$ and $B \subseteq C$. Show that $A \subseteq C$.

5. Show that if A and B are sets and $A \subset B$, then $|A| \leq |B|$.

6. Show that if A and B are sets where $|A| = |B|$, then $|\mathcal{P}(A)| = |\mathcal{P}(B)|$

7. Show that if A, B, and C are sets such that $|A| \leq |B|$ and $|B| \leq |C|$, then $|A| \leq |C|$.

(3.2) – Inclusion Proofs

Now that we have laid the foundation for dealing with sets and subsets, it is time to prove certain properties of sets. This chapter will deal with the relationship between various subsets, and whether two seemingly different sets are actually the same. We start, as always, with some defintions.

Definition- Let A and B be sets. The **UNION** of A and B, $A \cup B$, is the set that contains all of the elements in A and all the elements in B.

Definition- Let A and B be sets. The **INTERSECTION** of A and B, $A \cap B$, is the set of elements that are in both A and B.

Note that the intersection of two sets is a subset of the union of those sets. It is also important to note that the concept of a union or intersection can be extended to cover more than two sets. For example, the intersection of five sets would be the set of elements that belongs to each of the five sets. This may be a bit confusing, so it is best to look at some examples.

Given $A = \{1, 2, 3, 4, 5\}, B = \{3, 4, 6, 7, 9, 10\}, C = \{2, 5, 8\}$, find:

1. $A \cup C$
2. $A \cap B$
3. $A \cup B \cup C$
4. $A \cap B \cap C$

Before giving the solutions to these examples, we would be remiss if we failed to mention *Venn Diagrams*, or pictorial representations of sets. A Venn Diagram partitions sets in such a way to make it easy to see every union and intersection therein. Another benefit of the diagram is its ability to corroborate any inclusion proof you might complete. It is often easier to see the relationsihp between sets when they are all clearly drawn on paper. In general, when you are dealing with either two or three sets, your Venn Diagrams will consist of overlapping circles. As the number of sets increases, so does the complexity of the shapes needed to convey every relationship between those sets.

1. Any element in either A or C is in this set. $A \cup C = \{1, 2, 3, 4, 5, 8\}$
2. We want only the elements that belong to both A and B. $A \cap B = \{3, 4\}$.

3. $A \cup B \cup C = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

4. $A \cap B \cap C = \emptyset$

The only example that might require explanation is (4). You should note that while neither $A \cap B$ nor $A \cap C$ is empty, when we try to take the intersection of all three, we are left with nothing. There is no single element that is in all three sets. As a matter of fact, once we ask for the intersection of B and C, it doesn't matter what other sets are involved. Since there is no element in both B and C, any intersection involving those two sets will be empty.

Definition- Two sets are **DISJOINT** if their intersection is the empty set.

So B and C in the above example are disjoint. A is disjoint with neither of those two sets. If there are more than two sets in which no two sets share an element, we say those sets are *mutually disjoint*. A, B, C are NOT mutually disjoint because A shares elements with both B and C.

Definition- Let A, B be two sets. The **DIFFERENCE** of A and B, $A - B$, is the set containing all of the elements of A that are not contained within B.

The notation is a "minus" sign for a reason- the difference set is analagous to arithmetic subtraction, where $A - B$ takes all of the elements of A and then eliminates those elements that also reside within B. Here are two quick examples:

$A = \{1, 3, 4, 5\}, B = \{1, 2, 3\}$

1. $A - B = \{4, 5\}$ We want all elements that are in A but not B. Note that we don't care about the elements in B that are not in A.

2. $B - A = \{2\}$ This is simply the reverse of the process we applied in (1).

Definition- The **UNIVERSAL SET**, U, is the set of all objects in a given problem. Every other set in that particular problem is a subset of U.

Definition- Let U be the universal set. The **COMPLEMENT** of A, A^c, is equal to $U - A$.

Now that we have introduced the concept of the universal set, we will have to frame many of our questions within the context of that definition. Basically, you cannot figure out a complement unless you know what the universal set for that problem is. These examples show why.

1. $U = \{1, 2, 3, 4, 5\}, A = \{1, 2, 3\} \longrightarrow A^c = \{4, 5\}$
2. $U = \{1, 4, 9, 16\}, A = \{y : x \in \mathbb{Z}, 1 \leq x \leq 4, y = x^2\} \longrightarrow A^c = \emptyset$
3. $U = \mathbb{Z}, A =$ all odd integers $\longrightarrow A^c =$ all even integers

We are SO close to finally doing those inclusion proofs that I've been mentioning for two chapters. But before we get there, we want to mention a few facts about intersections and unions of important sets. These should be intuitive, or at the very least become clear after seeing their representations as Venn Diagrams.

1. $A \cap U = A \Longrightarrow$ Because $A \subseteq U$, the elements shared by both sets are simply A.
2. $A \cup U = U \Longrightarrow$ There are no elements in A that are not in U so the union is simply U.
3. $A \cap \emptyset = \emptyset \Longrightarrow$ The empty set contains no elements, so cannot share elements with A.
4. $A \cup \emptyset = A \Longrightarrow$ The empty set contributes no elements to the union, leaving only A.
5. $A \cup A = A \Longrightarrow$ All elements in both A and A gives us A.
6. $A \cap A = A \Longrightarrow A$ shares all elements with itself.
7. $(A^c)^c = A \Longrightarrow$ We can use the definition of complement for this one. $(A^c)^c = (U - A)^c = U - (U - A) = A$

THEOREM (3.2.1)- $A - B = A \cap B^c$
Proof- We stated earlier that the way to prove two sets are equal is to do a double inclusion. That means we have to show $A - B \subseteq B^c$ and $B^c \subseteq A - B$. This is how we do it:
$\Longrightarrow$

$$x \in A \cap B^c \tag{1}$$

$$x \in A, x \in B^c \tag{2}$$

$$x \notin B \tag{3}$$

$$x \in A, x \notin B \rightarrow x \in A - B \tag{4}$$

$\Longleftarrow$

$$x \in A - B \tag{5}$$

$$x \in A, x \notin B \tag{6}$$

$$x \in B^c \tag{7}$$

$$x \in A \cap B^c \tag{8}$$

First, we will give an explanation for the steps above:

(1) We take a random element from $A \cap B^c$.
(2) By definition of intersection, we know that x is both in A and B^c.
(3) By definition of complement, if $x \in B^c$, then $x \notin B$.
(4) $x \in A, x \in B^c$, so use the defintion of the difference of sets.

This completes the left to right inclusion.

(5) We take a random element from $A - B$.
(6) By definition of difference, $x \in A, x \notin B$.
(7) Definition of complement of B
(8) Definition of intersection

This completes the right to left inclusion.

■

Essentially, what we've done is show that if an arbitrary element called x is in the set $A - B$, that same element is in $A \cap B^c$, and vice versa. Because x is arbitrary, this holds for EVERY single element in each set. Thus we have proven that the two sets are the same. Again, a simple Venn Diagram will show this relationship in a very apparent way. In the future, we will not delineate every single step in an inclusion proof. It will be up to you to figure out why it is we take the steps we take.

THEOREM (3.2.2)- $A \cup B = B \cup A$
Proof- $\Longrightarrow x \in A \cup B$, so $x \in A$ or $x \in B$. Order of inclusion does not matter, so this means that $x \in B$ or $x \in A$. This is the very definition of the union of two sets. The $\Longleftarrow$ inclusion is done in the same exact way.

■

We can prove the same fact for intersections in an identical fashion. The next proof(s) we would like to tackle appear again and again in more advanced mathematics courses. Honestly, there's a good chance that if you go onto take classes in graduate level mathematics, you will see these two proofs in each of them. They are called:

THEOREM (5.3.3): DeMORGAN'S LAWS

(1) $(A \cap B)^c = A^c \cup B^c$

(2) $(A \cup B)^c = A^c \cap B^c$

Proof (1)
$\Longrightarrow x \in (A \cap B)^c \to x \notin (A \cap B)$. So $x \notin A$ and B. This means that x is either not in A or $x \notin B$. So $x \in A^c$ or $x \in B^c \to x \in (A^c \cup B^c)$
$\Longleftarrow x \in (A^c \cup B^c) \to x \in A^c$ or $x \in B^c \to x \notin A$ or $x \notin B \to x \notin (A \cap B) \to x \in (A \cap B)^c$

Q.E.D.

We leave it as an exercise to prove (2). Let's try a final proof that involves more than just two sets.

THEOREM (5.3.4)- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
Proof
$\Longrightarrow x \in A \cup (B \cap C) \to x \in A$ or $x \in (B \cap C)$. If $x \in (B \cap C) \to x \in B$ or $x \in C \to x \in A$ or $x \in B, C \to x \in A$ or B and $x \in A$ or $C \to x \in (A \cup B) \cap (A \cup C)$

■

As you will see throughout these notes, the second part is left for an exercise.

Before we mention one last thing and end the chapter, it makes sense to recap the process that we have applied to these inclusion proofs:
(1) Make sure you do two inclusions, a right-left, and a left-right.
(2) Take an arbitrary element (call it x) and assume it is an element of the left set.
(3) Use set theoretic definitions to establish that x is in the set on the right.
(4) Repeat the same process going in the other direction, proving that if x is in the set on the right, it must be in the set on the left.
(5) If you are having troulbe seeing the relationship between the two (or more) sets, a Venn Diagram might be useful in giving you a hint.

Also remember that once you have proven a theorem, you are free to use it to prove more difficult inclusion proofs. As an example, DeMorgan's two laws are often used to simplify complex-seeming sets so that a proof can be easily handled.

Most of the proofs we have contain two sets, but you have also seen examples which involved three or more sets. We will now introduce the shorthand notation that is used when we wish to represent a multitude of sets.

(1) $A_1 \cup A_2 \cup A_3 \cup ..... \cup A_n = \cup_{i=1}^{n} A_i$
(2) $A_1 \cap A_2 \cap A_3 \cap ..... \cap A_n = \cap_{i=1}^{n} A_i$

examples:

1. $A_i = \{1\}, \{1, 2\}, \{1, 2, 3\}, ...\{1, 2, 3, ..., i\}$
   (a) What is the set $\cap_{i=1}^{\infty} A_i$?
   (b) What is the set $\cup_{i=1}^{\infty} A_i$?
2. $A_i = [1, 1 + \frac{1}{i}]$
   (a) $\cap_{i=1}^{\infty} A_i =?$
   (b) $\cup_{i=1}^{\infty} A_i =?$

As usual, students should attempt to answer these questions on their own before looking at the answers. Have you answered them? You haven't? Well then you really shouldn't look below.

1. (a) The first thing to do in this type of question is to figure out what the sets look like. $A_1 = \{1\}, A_2 = \{1\}, \{1, 2\}, A_3 = \{1, 2, 3\}$...... Now, since we are attempting to find an intersection, we only care about the elements that are in EACH of the sets. The only element in each set is $\{1\}$.
   (b) Now we want to combine all of the elements that appear in ANY of the sets. As i increases by one, the set increases to include one more term than the previous entry. Since i ranges from 1 to ∞, the union of these sets is $\mathbb{Z}^+$. As an aside, we also note that $\forall j : A_j \subseteq A_{j+1}$
2. (a) Let's write out this problem in longhand: $\cap_{i=1}^{\infty} A_i = [1, 1\frac{1}{2}] \cap [1, 1\frac{1}{3}] \cap .....$ Note that these sets are intervals on the real number line, and so our solution will be the same. We want only the elements that appear in each of the sets. Since $\lim_{i \to \infty} 1\frac{1}{i} = 1$, we are approaching the set [1,1] as i approaches infinity. Thus, the intersection is [1].
   (b) We are looking at the same group of sets, but this time we want to include every single number that appears in any of the sets. In this case, the union is $[1, 1\frac{1}{2}]$.

Exercises

1. Let A=(1,2,3,4,5) and B=(0,3,6). Find:
   (a) $A \cup B$
   (b) $A \cap B$
   (c) A-B
   (d) B-A

2. Let A=(a,b,c,d,e) and B=(a,b,c,d,e,f,g,h). Find the same things I asked you to find in the previous question.

3. Find the sets A and B if A-B=(1,5,7,8), B-A=(2,10), and $A \cap B$=(3,6,9).

4. Draw Venn diagrams for each of these combinations of sets A, B, and C.
   (a) $A \cap (B \cup C)$
   (b) $A^c \cap B^c \cap C^c$
   (c) $(A - B) \cup (A - C) \cup (B - C)$
   (d) $A \cap (B - C)$
   (e) $(A \cap B) \cup (A \cap C)$
   (f) $(A \cap B^c) \cup (A \cap C^c)$

5. What can you say about sets A and B if we know that:
   (a) $A \cup B = A$
   (b) $A \cap B = A$
   (c) A-B=A
   (d) A-B=B-A

6. Let A and B be sets. Show that:
   (a) $(A \cap B) \subseteq A$
   (b) $A \subseteq (A \cup B)$
   (c) $(A - B) \subseteq A$
   (d) $A \cap (B - A) = \emptyset$
   (e) $A \cup (B - A) = A \cup B$

7. Let A, B and C be sets. Show that

   (a) $(A \cup B) \subseteq (A \cup B \cup C)$

   (b) $(A \cap B \cap C) \subseteq (A \cap B)$

   (c) $(A - B) - C \subseteq A - C$

   (d) $(A = C) \cap (C - B) = \emptyset$

   (e) $(B - A) \cup (C - A) = (B \cup C) - A$

8. Let A, B, and C be sets. Show that (A-B)-C=(A-C)-(B-C).

We've spent the past two sections on dealing with sets. Although you will encounter sets and make use of them in many future courses, for the most part, we will not need to use some of the more advanced set theoretic techniques. We did, however, need to establish many of the concepts of the previous section in order to fully explore the ideas we focus on in this section. You all have a general understanding of functions from high school math courses. You were told that if a graph passes the "vertical line test", then it is a function. You may have been given other defintions, but this is probably the first thing you think when you think about functions. You will soon learn that many of the definitions you may have learned in high school left out some very important points that are vital in fully understanding just what a function is.

(3.3) – Functions

Definition- Let A, B be sets. A **MAPPING** from A to B, $A \to B$, is a pairing of elements in A with elements in B.

Depending on what the sets A and B are, a mapping can give you some strange objects. Mostly, however, mappings produce ordered pairs of numbers, where the first element of the ordered pair comes from set A and the second element of the ordered pair comes from set B. $(1,2), (\sqrt{6}, -1.2), (10, Red)$ would be examples of ordered pairs resulting from a mapping from A to B.

Definition- A, B sets. A **FUNCTION** $f : A \to B$ is a mapping where every element of set A corresponds to a single element in set B.

A few things about this definition. First and foremost, this probably differs from your high school definition in that it involves actual sets, instead of just some vague concept of a vertical line test (VLT). At the same time, this definition meshes with the idea of the vertical line test in that there is no element from set A that corresponds to more than one element from set B. Perhaps it is important to see why this is.

There are two criteria in the definition of a function that we must observe. The first is that EVERY element $a \in A$ has a corresponding value in B, called $f(a)$. We will explore this a bit later, but suffice to know that a mapping may or may not be a function depending on what A is. The second thing we care about is making sure that each $a \in A$ corresponds to ONLY one $f(a)$. Let's look at the specific case of a graph on the xy (cartesian) coordinate plane, keeping in mind that a typical element of this mapping would be of the form (a, b), where $a \in A$ and $b \in B$. These are the *ordered pairs* that you are so familiar with from high school.

The first question we should be asking is, what is our set A and what is our set B in this case? The xy plane is a visual representation of a mapping from the real numbers to the real numbers, so both A and $B = \mathbb{R}$. We can restrict our sets to cover only $\mathbb{R}^+$ or $(-3, 5)$, for example, but on a graph, we will always be dealing with real numbers. Now that we understand how to translate sets onto a graph, we can see how the vertical line test works. Assuming that we are dealing with a mapping that exists over all of set A, we can look at what it means to have two values in B correspond to a single element in A. If this were the case, and since $B = \mathbb{R}$, we would have two values in B, call them s, t such that $f(a) = s$ and $f(a) = t$. This gives us two ordered pairs (a, s) and (a, t). Plotting these two points on a graph gives us two points on the vertical line $x = a$, and the vertical line test has failed.

ex: Is $f(x) = \sqrt{x}$ a function? It does pass the vertical line test, but we know that isn't sufficient anymore to determine whether or not a mapping is a function. One problem we have is that we don't know what set we are mapping from or what set we are mapping to. We often cannot answer the question of whether or not $f : A \to B$ is a function without first knowing what sets A and B are. In this example, we were not given A or B, but we really only care about A. If $A = \mathbb{R}^+$, then f is a function. If $A = \mathbb{R}$, then f is not a function, because not EVERY element in the set has a corresponding value in B.

ex: Is $f(x) = x^2$ a funtion? YES! No matter how you restrict your set A, f exists over every element of that set. You may have noticed that we have not yet used the terms *domain* and *range*, but basically when your concept of domain is all real numbers, we will always have a function so long as the vertical line test holds. Since the VLT holds for this mapping, f is a function.

ex: Is $x^2 + y^2 = 4$ a function if.....

1. $A, B = \mathbb{R}$? NO. You may recognize this as the graph of a circle centered at the origin with a radius of 2. This mapping does not pass the vertical line test.

2. If the mapping is confined to Quadrants I and II? NO. Although it passed the VLT, there is corresponding B value for $x = -5$.

The examples thus far have involved sets of real numbers that can easily be seen as ordered pairs on a typical graph. The sets in question, however, can be more abstract, and the VLT is rendered meaningless.

ex: $A = \{a, b, c, d, e\}, B = \{a, b, c, d\}$. Are the following functions?

1. $f(a) = b, f(b) = c, f(c) = a, f(e) = d$. NO. d doesn't have a corresponding element $f(d)$ in set B.
2. $f(a) = a, f(b) = a, f(c) = a, f(d) = a, f(e) = a$. YES. Every element in A corresponds to a single element in B.

So as a quick recap, to test if a mapping is a function, we need to check only two things. The first is that every element in set A is "covered", and second is that no element in A corresponds to two different values in B.

Definition- A function $f : A \to B$ is **ONE-TO-ONE** or **INJECTIVE** if $\forall x, y \in A : f(x) = f(y) \longrightarrow x = y$.

All the symbols in that definition are known, but perhaps the translation is a bit difficult. This says, "For all x and y in the set A, the fact that $f(x)$ is equal to $f(y)$ implies that x is equal to y". Sorry if you were able to get there on your own.

Before we attempt to use the definition to prove functions are one-to-one algebraically, it might be helpful to give the graphical interpretation of this concept. Just as functions must pass a vertical line test, one-to-one functions must pass a "horizontal line test" (HVT). The reason for this should be clear. If a function does not pass the HVT, it means that there are two different elements in set A that correspond to the same element in set $b \in B$. This tells us that $f(a_1) = b = f(a_2)$. But $a_1 \neq a_2$, so f is not one-to-one.

Try to determine whether the following functions are one-to-one:

1. $f : \mathbb{R} \to \mathbb{R}, f(x) = -x^3$
2. $f : \mathbb{R} \to \mathbb{R}, f(x) =log(x)$
3. $f : \mathbb{R} \to \mathbb{R}, f(x) = x^3 - x$
4. $A = \{a, b, c, d\}, B = \{e, f, g, h\}$ $f(a) = e, f(b) = f, f(c) = g, f(d) = h$

1. This function passes the horizontal line test, so it is one-to-one.
2. This one was a trick question. It isn't even a function, because not every element $x \in \mathbb{R}$ has a corresponding $f(x)$. For example, there is no $f(-3)$, so f certainly isn't one-to-one.

3. This one doesn't pass the horizontal line test either, but it might not be so easy to see on a graph if you are using a calculator. So let's look at $f(0)$ and $f(1)$. Both of them are equal to 0. This tells us that we have two different elements in A that map to the same element in B. So f is not one-to-one.

4. We cannot use the HLT for this one. But we know by the defintion, that if $f(x) = f(y)$, then x should equal to y. Because we have no repeat element $f(x)$, this function is one-to-one.

Now we will show how to prove that a function is one-to-one algebraically. For the purpose of these exercises, we will modify the definition ever-so-slightly to "If $f(a) = f(b) \to a = b$.

<u>ex</u>: $f(x) = 2x - 3$. We know that this is a function regardless of what set we map this over. We also know that this is a one-to-one function because every linear function is one-to-one. But we are tasked to find this out algebraically. So we apply the definition: Start by claiming that $f(a) = f(b)$. So $2a - 3 = 2b - 3$. Now perform the algebraic steps (subtract 3 and divide 2) to solve for a.

<u>ex</u>: $f(x) = x^2 + 2x$ Always start with $f(a) = f(b)$. So $a^2 + 2a = b^2 + 2b$. We will complete the square by adding 1 to each side, giving us $a^2 + 2a + 1 = b^2 + 2b + 1$ or $(a + 1)^2 = (b + 1)^2$. Taking the square root of both sides yields $a + 1 = \pm(b + 1)$. This results in two solutions: $a = b$ and $a = -b - 2$. Thus, when $f(a) = f(b)$, a does not necessarily equal b.

<u>ex</u>: $f(x) = |x| \to |a| = |b| \to a = \pm b \to f$ is not one-to-one.

<u>ex</u>: $f(x) = \lceil x \rceil \to \lceil a \rceil = \lceil b \rceil$ This is where it gets a bit tricky. We know that $\hat{a} = \lceil a \rceil$ implies that $a - 1 < \hat{a} \leq a$, and $\hat{b} = \lceil b \rceil$ implies that $b - 1 < \hat{b} \leq b$. This gives us a range for both a and b, meaning that a does not necessarily equal b.

<u>**Definition**</u>- A function $f : A \to B$ is **ONTO** or **SURJECTIVE** if $\forall b \in B, \exists a \in A$ such that $f(a) = b$.

That's definitely a little confusing, so here is a way to understand the definition in english: *EVERY element in set B is hit by an element in set A.* To break it down further, this simply means that there is no element in set B that doesn't have a corresponding element in set A.

<u>ex</u>: $f : \mathbb{R}^+ \to \mathbb{R}^+ : f(x) = \frac{1}{x}$ This function is onto because there is no restriction on set B. $B = \mathbb{R}^+$, and every single element in $\mathbb{R}^+$ can be hit by plugging its reciprocal into the function.

ex: Is $A = \{a, b, c, d\}, B = \{a, b, c, d\}$, $f(a) = d, f(b) = c, f(c) = b, f(d) = d$ an onto function? NO, because there is an element in B that does not have a corresponding element mapped from A. That element is a.

ex: Show that $y = 3x + 7$ is onto algebraically. This function is not onto if there is a y value that is not "hit". The way we can determine whether or not this is true is by solving for x, and seeing if there are any restrictions on the resulting equation. In this case, we get $x = \frac{y-7}{3}$. Since y can take on any value without a "problem", the function is onto.

ex: Is $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2 - 13$ onto? Well if $y = x^2 - 13$, then $x = \sqrt{y + 13}$, and there ARE restrictions on y. If $y < -13$, then x does not exist. So f is not onto.

Definition- A function that is both injective and surjective is called a **BIJECTION**.

Figuring out whether or not a function is a bijection is as simple as performing the tests for onto and one-to-one. You will find that bijections are very important because they have *inverses*, or functions that allow us to reverse the original.

Exercises

1. Why is f NOT a function from $\mathbb{R}$ to $\mathbb{R}$?

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

   (b) $f(x) = \sqrt{x}$

   (c) $f(x) = \pm\sqrt{x^2 + 1}$

   (d) $x = 3 - y^2$

2. Determine whether f is a function from $\mathbb{Z}$ to $\mathbb{R}$ if:

   (a) $f(n) = \pm n$

   (b) $f(x) = \sqrt{x^2 + 1}$

   (c) $f(x) = \frac{1}{x^2-9}$

3. Determine whether or not each of the following functions is one-to-one:

   (a) $f(a) = b, f(b) = a, f(c) = c, f(d) = d$

   (b) $f(a) = b, f(b) = b, f(c) = d, f(d) = c$

(c) $f(a) = d, f(b) = b, f(c) = c, f(d) = d$

4. Determine whether or not the functions in question 1 are onto.

5. Prove the following are one-to-one (or not) algebraically:

   (a) $|x - 2| = y$

   (b) $y = 7x - 5$

   (c) $\frac{1}{x-1}$

   (d) $x^2 - 6x + 2$

   Give an example of a function from $\mathbb{Z}^+ \to \mathbb{Z}^+$ that is

   (a) one-to-one but not onto

   (b) onto but not one-to-one

   (c) both onto and one-to-one

   (d) neither onto nor one-to-one

6. Determine whether each of the following functions is a bijection from $\mathbb{R} \to \mathbb{R}$:

   (a) $f(x) = -3x + 4$

   (b) $f(x) = -3x^2 + 7$

   (c) $f(x) = \frac{x+1}{x+2}$

   (d) $y = x^5 + 1$

   (e) $f(x) = \frac{x^2+1}{x^2+2}$

Switching gears just a bit, we are going to introduce a concept that is prevalent throughout mathematics, namely the equivalence relation. As the name implies, these are special relationships between members of a set, and are foundation for many more complicated structures in advanced mathematics.

(3.4) – Equivalence Relations

We have to build up to the concept of an equivalence relation by giving some definitions.

Definition- Let A and B be sets. A **BINARY RELATION** from A to B is an ordered pair (a, b) where $a \in A$ and $b \in B$. We can group some (or all) of these ordered pairs (a, b) to form a new set that we will call R.

That's a rather abstract definition. All we are saying about a relation right now is that it relates elements in one set to element in another set. When those two elements are related, they form another set, which we call R.

ex: Let $A = \{1, 2, 3\}$ and $B = \{a, b\}$. Then a relation between A and B is $R = \{(1, a), (2, a), (2, b), (3, b)\}$. In this case, we can say $1Ra$ but it is not true that $3Ra$.

ex: Let $A = \{1, 2, 3, 4\}$. We can create a relation from A to itself with the rule: $R =\{(a_1, a_2)|a_1$ divides $a_2\}$. The relation yields the following pairs:
$1R1, 1R2, 1R3, 1R4, 2R2, 2R4, 3R3, 4R4$.

Q: Consider the following relations on $\mathbb{Z}$:

$R_1 = \{(a, b)|a \leq b\}$

$R_2 = \{(a, b)|a > b\}$

$R_3 = \{(a, b)|a = b \text{ or } a = -b\}$

$R_4 = \{(a, b)|a = b\}$

$R_5 = \{(a, b)|a = b + 1\}$

$R_6 = \{(a,b)|a+b \leq 3\}$

Which of these relations contain each of the pairs (1,1),(1,2),(2,1),(1,-1) and (2,2)?

Ans: The pair (1,1) is in R_1, R_3, R_4 and R_6; (1,2) is in R_1 and R_6; (2,1) is in R_2, R_5, R_6; (1,-1) is in R_2, R_3 and R_6; (2,2) is in R_1, R_3, R_4.

Definition- A relation R on set A is called **REFLEXIVE** if $\forall a \in A : (a,a) \in R$.

ex: Which relations from Q are reflexive?
Ans: Any one of them where (a,a) is a member or R_i. So, R_1, R_3, R_4.

ex: Is the relation "multiplication" reflexive on the integers?
ans: If we take an integer a and multiply it by itself, do we get back an integer? Yes! $\forall a \in \mathbb{Z} : a^2 \in \mathbb{Z}$.

Definition- A relation R on a set A is called **SYMMETRIC** if $\forall a_1, a_2 \in A$: $(a_2, a_1) \in R$ whenever $(a_1, a_2) \in R$.

ex: Which relations in Q are symmetric?
ans: Going by the definition, we should assume that $(a_1, a_2) \in R$, and then see if $(a_2, a_1) \in R$. This is only true for R_3, R_4, R_6.

ex: Is the relation "division" symmetric on the integers?
ans: No. Take the ordered pair (4,2), which is in the set R (because 4 divided by 2 is 2, which is an integer). If (4,2) were symmetric, (2,4) would be in R. But when you divide 2 by 4, you get .5, which is not an integer.

Definition- A relation R on set A is called **TRANSITIVE** if $\forall a, b, c \in A$: whenever $(a,b) \in R$ and $(b,c) \in R$, then $(a,c) \in R$.

ex: Which relations in Q are transitive?
ans: By definition, we are given that $(a,b) \in R$ and $(b,c) \in R$. We just need to check that $(a,c) \in R$. This is true in R_1, R_2, R_3, R_4.

ex: Is division transitive on the integers?
ans: Well, if a divides b and b divides c, is it true that a divides c? We cannot prove this yet, but plugging in numbers should convince you that this works for all a, b, c when the given conditions hold.

Finally! We are ready to give the definition for an equivalence relation now, but let's make a quick note. Going back to Q from earlier, it is important to recognize that R_3, the equality relation, was reflexive, symmetric and transitive. Maybe that comes as no surprise, because an equality is the "strongest" relation that can exist between two elements. Now.....

Definition-A relation on set A is called an **EQUIVALENCE RELATION** if it is reflexive, symmetric and transitive.

So, as we just stated, the equality relation is an equivalence relation on any set.

Definition- Elements a and b that are related by an equivalence relation are said to be **EQUIVALENT**. The notation $a \sim b$ is used to denote that a and b are equivalent elements with respect to a particular equivalence relation.

ex: Let R be the relation on the set of integers where $(a, b) \in R$ when $a - b \in \mathbb{Z}$. Is R an equivalence relation?
ans: We need to check the three conditions of an equivalence relation. R is obviously reflexive, because $a - a = 0$ is always an integer. To check symmetry, we start with the assumption that $a - b \in \mathbb{Z}$. Now what about $b - a$? Well, if $a - b = k$, then $b - a = -k$. Since k was an integer by assumption, $-k$ is as well. Finally, transitivity: we assume $a - b, b - c \in \mathbb{Z}$. Look at $a - c$- We can say $a - b = k$ so that $b = a - k$. Now, let's say that $b - c = l$ (where k, l are integers by assumption) and replace b to get $a - k - c = l$. That gives us $a - c = k + l$, which is also an integer, and our test is done. R is an equivalence relation.

ex: Let R be the relation on the set of real numbers such that xRy if and only if$x$ and y are real numbers that differ by less than 1. Is this an equivalence relation?
ans: R is reflexive, because $x - x = 0 < 1$. It is also symmetric because given x-y¡1, we know that the distance between x and y is less than 1. This implies that $|y - x| < 1$. Transitive is where this relation fails the equivalence test. Simply choose $x = 0, y = .5, z = 1$ and you will see that $|x - z| \not< 1$.

As you can see, to prove that a relation is NOT an equivalence relation, simply find a counterexample that "breaks" one of the there criteria. This is no different than when you found counterexamples to disprove potential faulty theorems.

Definition- Let R be an equivalence relation on set A. The set of all elements that are related to an element $a \in A$ is called an **EQUIVALENCE CLASS** of a. Another way to say this is that the equivalence class of a is equal to $\{\forall b : (a, b) \in R\}$.

ex: Consider the equivalence relation R where $(a, b) \in R$ if a and b yield the same

remainder when divided by 4. (You will verify that this is an equivalence relation as an exercise) What is the equivalence class of the number 15?
ans: Two numbers are equivalent if they give the same remainder when divided by 4. What remainder does 15 yield when divided by 4? A quick computation tells us 3, so that any other integer that yields a remainder 3 will be in its equivalence class. So the solution is $\{.... - 4, -1, 3, 7.....\}$.

One very important fact about equivalence relations is that they *partition* the set in which they are contained. A partition is a collection of non-empty, disjoint subsets that have the entire set as their union. To put in plainer terms- every element in the overall set is in one of the subsets, and no element is in more than one. Looking back at our previous example, we can see that the relation splits the integers into four disjoint subsets. Those subsets can be thought of as the numbers that yield remainders 0,1,2 and 3 when divided by 4.

Exercises

1. If $A = \{a, b, c\}, B = \{0, 1, 2\}$, create a relation R that yields the largest resulting set.
2. Which of the following are equivalence relations on the set $\{0, 1, 2, 3\}$?
   (a) $\{(0, 0), (1, 1), (2, 2), (3, 3)\}$
   (b) $\{(0, 0), (0, 2), (2, 0), (2, 2), (2, 3), (3, 2), (3, 3)\}$
   (c) $\{(0, 0), (1, 1), (1, 2), (2, 1), (2, 2), (3, 3)\}$
   (d) $\{(0, 0), (1, 1), (1, 3), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)\}$
   (e) $\{(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2), (2, 0), (2, 2), (3, 3)\}$
3. For those in the previous question that are not equivalence relations, determine which properties they lack.
4. Let R be the relation on the set of all real numbers such that SRT if and only if S and T have the same cardinality. What is the equivalence class of the set $\{0, 1, 2\}$ and $\mathbb{Z}$?
5. Let A be the set of ordered pairs of points on the xy coordinate plane, and let R be the relation defined as $(a, b) \in R$ if and only if a and b are two points on a line passing through the origin. Is R and equivalence relation? If so, prove it. If not, show which properties fail.

6. Suppose f is a function that has A as its domain. Let R be the relation on A consisting of all ordered pairs (x, y) such that $f(x) = f(y)$. Show that this is an equivalence relation on A. What are the equivalence classes of R? Let R be the relation on the set of all ordered pairs of positive integers such that $(a, b), (c, d) \in R$ if and only if $a + d = b + c$. Show that R is an equivalence relation.

7. Let R be the relation on the set of all ordered pairs of positive integers such that $(a, b), (c, d) \in R$ if and only if $ad = bc$. Show that R is an equivalence relation.

8. What are the equivalence classes of R in the previous question if $a, b, c, d \in \mathbb{R}$?

9. Show that the relation R on the set of differentiable functions from $\mathbb{R}$ to $\mathbb{R}$ consisting of all pairs of functions f, g such that $f'(x) = g'(x)$ is an equivalence relation. What functions are in the equivalence class of $f(x) = x^2$?

10. Which of these are partitions of $\mathbb{Z}x\mathbb{Z}$ (ordered pairs of integers)?

    (a) the set of pairs (x, y) where x or y is odd; the set of pairs (x, y) where x is even; the set of pairs (x, y) where y is even

    (b) the set of pairs (x, y) where both x and y are odd; the set of pairs (x, y) where exactly one of x and y is odd; the set of pairs (x, y) where both x and y are even

    (c) the set of pairs (x, y) where x is positive; the set of pairs (x, y) where y is positive; the set of pairs (x, y) where both x and y are negative

    (d) the set of pairs (x, y) where 3 divides both x and y; the set of pairs (x, y) where 3 divides x but 3 doesn't divide y; the set of pairs (x, y) where 3 doesn't divide x but 3 divides y; the set of pairs (x, y) where 3 doesn't divide x or y

    (e) teh set of pairs (x, y) where $x > 0, y > 0$; the set of pairs (x, y) where $x > 0, y \leq 0$; the set of pairs (x, y) where $x \leq 0, y > 0$; the set of pairs (x, y) where $x \geq 0, y \geq 0$

    (f) the set of pairs (x, y) where $x = 0, y \neq 0$; the set of pairs (x, y) where $x = 0, y \neq 0$; the set of pairs (x, y) where $x \neq 0, y = 0$

We've spent the the past few chapters learning techniques that will help us place certain mathematical forms in the abstract. We have taken concepts that we were once comfortable with and broken them down into components so we could see the underlying structures from which they are formed. That practice continues in this chapter as we take some arithmetic concepts that you may have taken for granted, and prove some very important facts about them.

(4.1) – Divisibility

Definition- An **INTEGER** is a number that can be written without a decimal or fractional component.

You could also say that an integer is simply a whole number. -7 is an example of an integer. π is not an integer.

Definition- $a, b \in \mathbb{Z}; a \neq 0$. We say a **DIVIDES** b, $(\mathbf{a}|\mathbf{b})$, if there is an integer c such that $b = ac$. In this case, we will say that b is a **MULTIPLE** of a, and a is a **FACTOR** of b.

ex: $7|91 \longrightarrow$ This is a TRUE statement because $7k = 91 \rightarrow k = 13 \in \mathbb{Z}$.

ex: $4 \nmid 34 \longrightarrow$ This means that 4 does not divide 34, which is apparent becasue $4k = 34 \rightarrow k = 8.5 \notin \mathbb{Z}$.

ex: $11|242 \longrightarrow$ This is a TRUE statement for the same, obvious reasons. There are many ways to prove that a number is divisible by 11. You could simply divide using a calculator, but that is no fun. In this case, you can also look at 2-4+2=0. Since 0 is divisible by 11, 242 is divisible by 11. If you did not know that "trick", don't worry- we will leave it for an exercise at the end of this section.

As you can see, the rules for divisibility have not changed- they are the same rules you have been using since 5th grade. The definition, while seemingly more complicated than the one to which you are accustomed, will allow us to prove many properties of divisibility that you never before knew you had been using.

THEOREM (4.1.1)

1. If $a|b, a|c \longrightarrow a|(b + c)$

2. If $a|b \longrightarrow a|bc \ \forall c \in \mathbb{Z}$

3. If $a|b, b|c \longrightarrow a|c$

We are encountering theorems based on new definitions, so the first thing we should do is figure out exactly what we are trying to prove. Let's start by putting them into english.

1. This says *If a divides b and a divides c, then a divides b plus c.* Easy enough, and we can plug in numbers to get a feel for whether or not it works. Let's say that $a = 9, b = 18$, and $c = 207$. This theorem states that since $9|18$ and $9|207$, then $9|225$. This is, of course, true.

2. *If a divides b, then a divides bc for all integers c.* We can make $a = 12, b = 60, c = 48$. Then $12|60 * 48 = 2880$.

3. *If a divides b and b divides c, then a divides c.* We will say $a = 6, b = 24, c = 72$. Then $6|24$, and $24|72$, so $6|72$.

Now let's prove these theorems in the abstract.

Proof

1. $a|b, a|c$ is given to us. If we apply the definition of division to these statements, we get $ak = b$ and $al = c$. Now, we want to prove the statement $a|(b + c)$, which if we were to apply the definition, would give $am = (b + c)$, where m can be any integer. So, we need $(b + c)$ on the left side of our proof equation. We can get this by adding our two equations $ak = b$ and $al = c$. This gives us $ak + al = b + c$, which can be rewritten $a(k + l) = b + c$. If we were to substitute $m = k + l$, then we get $am = b + c$. Now notice that this is the definition of division again, so $a|(b + c)$.

2. We have $a|b$ and want $a|bc$. So let's apply our definition to get $ak = b$ and multiply both sides by c. So $akc = bc$. Now replace kc with m and see that $am = bc$. By our definition of division, this means $a|bc$.

3. Given $a|b$ and $b|c$, this means $ak = b$ and $bl = c$. We can replace b in the second equality with ak to get $akl = c$. When we substitute m for kl, we get $am = c$, which by definition means $a|c$.

So we have proven some rules that we probably already knew. But now we know exactly why they work! Once you become comfortable with this type of proof, you can skip the step where you replace your variables with m. The only reason this was done above was to show you that our work conformed to the definition of division. The substitution is really unnecessary.

Corollary: $a, b, c \in \mathbb{Z}$ s.t. $a|b$ and $a|c$. Then $a|(mb + nc)$.

A corollary is a theorem that follows directly from previously proven theorems. Because we have already proven the components of this statement, it should be apparent why it is true.

ex: Prove by induction for $n \geq 0 : 5|(8^n - 3^n)$
We start with the basis case when $n = 0 : 5|8^0 - 3^0 \rightarrow 5|0$, which is true.
Now we replace n with k for our assumption: $5|(8^k - 3^k)$.
We want to prove our statement for $k + 1$, or that $5|(8^{k+1} - 3^{k+1})$ We will perform a little bit of "magic" to get this done. We know whe have to use the assumption, so let's add and subtract both 8^k and 3^k from the right side of the division sign. This gives us $5|(8^{k+1} - 3^{k+1} + 8^k - 8^k + 3^k - 3^k)$. We are allowed to do this because ultimately, we are just adding terms that sum to 0. Now let's rearrange our terms: $5|[(8^k - 3^k) + (8^{k+1} - 8^k - 3^{k+1} + 3^k)]$. We know from our previous theorem that if $a|b$ and $a|c$, then $a|(b + c)$, and that $5|(8^k - 3^k)$ from our assumption. This means that if we can prove that $5|(8^{k+1} - 8^k - 3^{k+1} + 3^k)$, then we have proven the entire statement. We should start by factoring out an 8^k and a 3^k, giving us $5|[8^k(8 - 1) - 3^k(3 - 1)]$ or $5|(7 * 8^k - 2 * 3^k)$. Break down the 7, giving us $5|(5 * 8^k + 2 * 5^k - 2 * 3^k)$. We know by our theorems that $5|5 * 8^k$, which means we now only have to prove that $5|(2 * 8^k - 2 * 3^k)$, or $5|[2(8^k - 3^k)]$. However, we know that $5|(8^k - 3^k)$, so we are done.

$\blacksquare$

Yeah, that was pretty intimidating, but it just goes to show how powerful our previous theorems are. It might seem silly that we can say that 5 ALWAYS divides $8^n - 3^n$, but it is true, and now you have proven it. There are many strange facts (some you already know!) that can be proven using only the theorems we proved earlier in this chapter, and the following.....

THEOREM (4.1.2)- If n is a positive integer, n can be expressed uniquely in the form $n = a_k * 10^k + a_{k-1} * 10^{k-1} + a_{k-2} * 10^{k-2} + ... + a_1 * 10 + a_0$, where k is a nonnegative integer, and a is a nonnegative integer less than 10. Furthermore, $a_k \neq 0$.

The proof of uniqueness is something we will leave for future courses on the subject, but the curious student can easily find all relevent information online (or by asking their teacher in extra help!). Oh, you aren't *that* curious? My bad. At any rate, we use this theorem when we wish to express an integer in terms of its digits. We call this process expressing an integer in **EXPANDED FORM**.

ex: $31704 = 3 * 10^4 + 1 * 10^3 + 7 * 10^2 + 0 * 10^1 + 4$

THEOREM (4.1.3)- The sum of the digits of a five-digit number N is divisible by 9 $\longleftrightarrow$ N is divisible by 9
Proof- This is a trick that many elementary school instructors teach their students in the lesson for division. If you add up the digits of a particular number, and the resulting sum is divisible by 9, then the number itself is divisible by 9. This is a fact that holds for any number, but we will prove it for five-digit numbers to save space.

$\Longrightarrow$ N is a five digit number that we will put in expanded form. $N = 10^4 * a + 10^3 * b + 10^2 * c + 10^1 * d + e$, where the digits of N are a, b, c, d, e. We are given that $9|(a + b + c + d + e)$, and want to prove that $9|N$. Let's write $N = 10000a + 1000b + 100c + 10d + e = (a + 9999a) + (b + 999b) + (c + 99c) + (d + 9d) + e = (a + b + c + d + e) + (9999a + 999b + 99c + 9d)$. We know by our given that 9 divides $(a + b + c + d + e)$, so now all we have to do is prove that $9|(9999a + 999b + 99c + 9d)$. We can see easily that $9|9(1111a + 111b + 11c + d)$, so our proof is done!

$\Longleftarrow$ This is basically the reverse of the previous part. Given $9|(10000a + 1000b + 100c + 10d + e)$, and the fact that $9|(9999a + 999b + 99c + 9d)$, we can see that $9|[|(10000a+1000b+100c+10d+e)-(9999a+999b+99c+9d)]$. So, $9|(a+b+c+d+e)$.

Q.E.D.

THEOREM (4.1.4): (Division Algorithm)- If a and d are positive integers, there exist unique integers q and r such that $a = dq + r$, $(0 \leq r < d)$

We will not prove that these numbers are unique in this text. It is more important to understand what the division algorithm is actually saying, and as it turns out, it is saying something you are very familiar with. Let's look at an example to explain:

ex: Find numbers q, r that fulfill the division algorithm is $a = 81$ and $d = 4$
We set up our equation: $81 = 4q + r$. It might seem like there are an infinite number of solutions for q and r, but this is not the case when you consider the last part of the theorem: $(0 \leq r < d)$. Since $r < d$, and $d \geq 0$, r can only take on the values $0, 1, 2, 3$. If r is any of those numbers but 1, q will not be an integer. So $r = 1$, and then we can solve for q to get $q = 20$.

ex: Do the same if $a = 237, d = 9$. $235 = 9q + r$ can be solved in the same way. The solution is $q = 26, r = 3$. Note that if we were to try $q = 25$ (or lower), we would end up with $r = 12$ (or higher), which is larger than $d = 9$. So there is only one possible answer.

Now this might seem like a lot of trial and error to get the solution, but perhaps you see the shortcut. We divide our d into a using long division, and find the quotient and the remainder. And this is what the division algorithm is showing us- that any two positive numbers can be expressed in terms of each other. The q that we find is the **QUOTIENT** and the r is obviously the **REMAINDER**.

THEOREM (4.1.5)- One of any three consecutive integers is divisible by 3.

Let's first see if this is even true. Take any three consecutive integers- 100, 101, 102. Yes, 102 is divisible by 3. One more try: 1097,1098,1099. 3 goes into 1098 (368 times). So it seems to be working. Now let's prove it.

Proof- We have three consecutive integers, so we will write them as $a, a+1$, and $a+2$. Looking at the number a, we can place it into the division algorithm with the number $d = 3$ to get $a = 3q + r$. We know that r has to be less than or equal to 2, which means $r = 0, 1, 2$. We will utilize a proof by cases for each of those r's.
case 1: $r = 0 \Longrightarrow$ This is the easy case. If $r = 0$, then $a = 3q$ and $3|a$.
case 2: $r = 1 \Longrightarrow$ If $r = 1 \longrightarrow a = 3q + 1$. This means that, when divided by 3, a gives you a remainder of 1. So, when 3 divides $a + 1$, it will give a remainder of 2. And, when 3 divides $a + 2$, it would normally give a remainder of 3. But we cannot get a remainder of 3, so this is what happens instead, according to the division algorithm: $a + 2 = 3(q + 1) + 0$. This means that $3|(a + 2)$.
case 3: $r = 2 \Longrightarrow$ If $r = 2 \longrightarrow a = 3q + 2$. The same thing occurs as in case 2, though this time, $3|(a + 1)$.

There were three possible cases for the number a- that it would yield a remainder of 0,1, or 2. In each of those cases, we were able to show that 3 divided either $a, a + 1$ or $a + 2$. Thus, given any three consecutive integers, one of them will be divisible by 3.

■

We will use these theorems over and over throughout this chapter. It is important to internalize these definitions early, as they are the basis for all of Number Theory.

Exercises

1. Without the use of a calculator, can you determine if the following are true?

   (a) $6|156$

   (b) $7|555$
   (c) $12|-1334$
   (d) $9|72-1116$
   (e) $14|21*100004$

2. Prove that if $a|b, a|c \longrightarrow a|(b-c)$

3. Prove that $\forall a : a|0$

4. Is it true that $0|a\ \forall a$? If so, prove it. If not, explain why.

5. Prove or disprove via counterexample: $a|(b+c) \longrightarrow a|b$

6. Prove by induction for $n \geq 0 : 3|(4^{n+3} - 3n - 10)$

7. Write the following numbers in expanded form: 47, 109, 3340, 8600057

8. How might you prove divisibility by 9 for an arbitrarily large number?

9. Prove: If the last two digits of a six digit number are divisible by 4, then the whole number is divisible by 4.

10. A **BINARY NUMBER** is an integer made up of only 0s and 1s. For example, 110111101 is a binary number. What is the smallest binary number divisible by 225?

11. Find q and r to fulfill the division algorithm:

    (a) $a = 100, d = 13$
    (b) $a = 567, d = 9$
    (c) $a = 378, d = 6$
    (d) $a = 40, d = 67$

12. Will the division algorithm work for negative ingtegers? Why or why not?

13. Prove that given five consecutive numbers, one of them will be divisible by 5.

14. Prove that given two consecutive even numbers, one of them will be divisible by 4.

15. Does 17 divide each of these numbers?: 68, 84, 357, 1001

16. Prove that if a is an integer other than 0, then

    (a) 1 divides a

   (b) a divides 0

17. Prove that if a, b, c, d are integers, where $a \neq 0$, such that $a|c, b|d$, then $ab|cd$.

18. Show that if a, b, c are integers, where $a, c \neq 0$, such that $ac|bc$, then $a|b$.

19. Show that if a is an even integer, then 2 divides a

20. Prove: If $a|b$ and $b|a$, where both a and b are positive integers, then $a = b$.

21. What is the quotient and remainder when

    (a) 19 is divided by 7?

    (b) -111 is divided by 11?

    (c) 789 is divided by 23?

    (d) 0 is divided by 9?

    (e) -1 is divided by 3

    (f) 4 is divided by 1

22. Prove: If $a|(b + c)$ and $a|c$, then $a|b$

23. If $p^a|m \longrightarrow p^{ka}|m^k$

24. Find a, b, c such that $a|bc$ but $a \nmid b$ and $a \nmid c$.

25. Prove or find a counterexample: $(a - b)|(a^2 - b^2)$

26. Can you find conditions for n under which the following will work? $n|a \to n|\frac{a^2}{2}$

27. When is it true that if $x \neq 0$, $8|(x^3 - 4x)$?

28. Prove by induction on k: $(n - 1)|(n^k - 1)$

29. Prove that 5 divides one of any five consecutive integers.

30. Prove that 3 divides one of any three integers $a, a + d, a + 2d$.

It may seem like divisibility is a strange place to start our tour of Number Theory, but many of the theorems in the previous section pave the way to complex proofs about prime numbers. This section will explore the relationship between numbers and their prime divisors. We will use these numbers to compute things such as the greatest common divisor and least common multiple. This will become important when we decide to use Number Theory to tackle "real life" problems.

(4.2) – Prime Numbers

Definition- An integer $p > 1$ is called **PRIME** if its only positive factors are 1 and p. An integer $c > 1$ that is not prime is called **COMPOSITE**.

We already know these definitions, but just to be sure, we can show a few examples. 14 is a composite numbers because it has factors of 7 and 2. 37 is a prime number because its only factors are 37 and 1. As a note, the number one is unique in that it is neither prime nor composite, but a **UNIT**.

FUNDAMENTAL THEOREM OF ARITHMETIC (4.2.1)- Every integer greater than 1 can be written uniquely as a product of prime factors. We write these factors in order of increasing size.

As you might've guessed, we won't prove this theorem, or any involving uniqueness. Here are some examples of how we write numbers to conform to the Fundamental Theorem of Arithmetic (FTOA).

1. $500 = 2^2 * 5^3$
2. $96 = 2^5 * 3^1$
3. $333 = 3^2 * 37^1$
4. $1001 = 7^1 * 11^1 * 13^1$
5. $2011 = 2011^1$

It's not always easy to figure out the prime factors of larger numbers. You probably learned a technique in elementary school called *factor trees*, whereby you keep "shaving" off factors until you shrink the number completely down to a final prime factor. But what happens in the case of 2011, when you have no idea whether or not prime factors exist? It's difficult to determine the smallest prime factor, when that factor could be three or four digits. There are ways to make this process easier, however.....

THEOREM (4.2.2)- If n is composite, then n has a prime factor $\leq \sqrt{n}$.
Proof- If n is composite, we can write it as $n = ab$, where a and b are factors of n. We want to prove that either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$. We will attempt to prove this by contradiction, so assume that $a > \sqrt{n}$ and $b > \sqrt{n}$. Then $n = ab > \sqrt{n}\sqrt{n} = n \rightarrow n > n$, which is, of course, ridiculous. So we have found our CONTRADICTION, which means that either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.
Now, this means that n has a factor that is less than the square root of n, but we don't yet know that that factor is prime. If either a or b is prime, then we are done. If neither is prime, by the FTOA, we know that each has a prime factor less than or equal to each. Thus, even if the factors are composite, we can find a prime factor of the composite that is also a factor of n.

$\blacksquare$

This theorem might not seem so useful at first glance. Why do we care that every composite has a prime factor less than its square root? Well, honestly we don't. The useful part comes when we take the contrapositive of this theorem, which of course, is logically equivalent.

THEOREM (4.2.3)- If an integer n is not divisible by a prime number less than or equal to $\sqrt{n}$, then n is prime.

We now have a pretty nice method for figuring out whether or not a number is prime. It isn't terribly useful for extremely large numbers, but it will get us pretty far. By our contrapositive theorem, we now know that all we have to do is check the factors of n less than or equal to $\sqrt{n}$. If none of those integers are factors of n, then n is prime.

ex- Is 149 a prime number? By our theorem, we need ONLY check the primes less than or equal to $\sqrt{149}$. We don't need to check any other numbers! So, $\sqrt{149} \sim 12.2$, so we should only check primes less than 12.2. The primes in question are 11,7,5,3, and 2. Simple division will show that none of these are factors of 149, and thus 149 is prime.

Of course this method is just as cumbersome if the number is large enough. For example, if we want to figure out whether or not 1234567 is prime, we would be dealing with all prime numbers less than or equal to $\sqrt{1234567}$, which is still a pretty large number. Speaking of which, how many primes do you think there are in existence? There are more than 10 primes, obviously, but are there more than 1,000,000? More than 1,000,000,000,000? You might suspect that there are an infinite number of primes, but is there a way to prove such a thing if it is true? Well, there are an infinite number of primes, and we can prove it. As a matter of fact, there are dozens of infinite primality proofs. For the sake of brevity, we will show two of them.

THEOREM (4.2.4)- There are an infinite number of primes.
Proof- We will prove this by contradiction and start by assuming there are a finite number of primes. We will call those finite primes $p_1, p_2, p_3, ..., p_n$. The next thing we will do is multiply all of those numbers together (you'll see why in a moment) to get $N = p_1 * p_2 * p_3 * ..... * p_n$. Now take the number N, and add 1 to it so that we have two separate numbers, N and $N + 1$. According to the fundamental theorem of arithmetic, we know that $N + 1$ has at least one prime factor, which we will call p_k. So $p_k|(N + 1)$. But remember that N is the product of ALL prime numbers, which must include p_k. So $p_k|N$. We know from our theorems last section that if $p_k|N$ and $p_k|(N+1)$, then $p_k|(N+1)-N = 1$. Now, if p_k divides 1, then p_k must be equal to 1. But p_k is supposed to be a prime number, and 1 is not prime. CONTRADICTION! So our assumption is not correct, and there are an infinite number of primes.

Q.E.D.

Most infinite prime proofs involve an argument similar to this one. We cannot prove the supposition directly, so in cases such as this we will always make the assumption that there are a finite number of primes and then derive a contradiction. In the rare case where we do not find a contradiction, we must figure out a way to generate new primes. Here is one such proof:

THEOREM (4.2.5)- There are an infinite number of primes.
Proof- Look at the following numbers, and assume p is prime:
$A_1 = p$
$A_2 = p + 1$
$A_3 = p(p + 1) + 1$
$A_4 = A_1 * A_2 * A_3 + 1$
$A_5 = A_1 * A_2 * A_3 * A_4 + 1$
We keep going on like that, multiplying each previous term together and then adding 1. Why? Because each new term CANNOT share a factor with any of the previous terms. Thus, because the FTOA ensures that every number has a prime factor, each new term generates a new prime factor. Since we can carry on this process ad infinitum, there must be an infinite number of primes.

■

Don't worry if you have trouble following the arguments in the previous two proofs. These can be difficult to understand because we are not given much to work with. It often helps to plug in numbers and see if they bear out the main idea of the proof.

GOLDBACH'S CONJECTURE- every even integer greater than 2 can be written as the sum of two primes.

So, what's a conjecture? It's something that the mathematical community has been unable to prove, and yet at the same time, we are very, very, very, very sure of its truth. Goldbach's Conjecture does not say that the primes are unique, only that they exist.

ex: Show that Goldbach's Conjecture holds for the following numbers: 14,20,100.

1. 20=13+7
2. 14=7+7=11+3
3. 100=97+3.....

As the number 14 shows, the primes can be the same or different, and there can be more than one way to write an even as a sum of two primes. Also note that there are many ways to write the number 100 as a sum of two primes. 53 and 47 is another possible pair, as is the pair 11 and 89.

Definition- The **GREATEST COMMON DIVISOR (GCD)**, of two integers a and b, $(\mathbf{a}, \mathbf{b})$, is the largest number that divides both a and b.

Again, this is a concept that you are probably pretty comfortable with. You were probably taught to make factor trees for the two numbers that you were given, and to pick out the prime numbers that they share. This is a legitimate way to figure out what a GCD is, but it is not the only way. Let's start with a few examples to get a feel for the definition.

ex: (12,45)=3
ex: (56,462)=14
ex: (34,81)=1

As stated earlier, the solutions to each example can be computed after setting up factor trees, and figuring out which primes are shared by both. In the case of (34,81), there is no shared prime factor, so the GCD is 1.

Definition- Integers a and b are **RELATIVELY PRIME** is $(a, b) = 1$.

ex: (48,72,132)=12

As you can see, we can find the GCD of more than just two integers. It may seem obvious how we would compute this number, but let's prove it anyway.

THEOREM (4.2.6)-$(a,b,c) = ((a,b),c)$
Proof- Let $S =$ the set of all numbers that are common factors of a, b, and c, and R is the set of all common factors of (a,b) and c. If $x \in S \rightarrow x|a, x|b, x|c$. This means that $x|(a,b)$, and so $x|((a,b),c)$. So $S \subseteq R$. Now, take $y \in R$, so $y|(a,b)$ and $y|c$. So $y|a, y|b, y|c \rightarrow y|(a,b,c)$. Thus $R \subseteq S$, and by our double inclusion $R = S$. Now, if both sets are the same, then the largest number in each set is the same. But the largest number in each set is the greatest common factor of the set. So $(a,b,c) = ((a,b),c)$.

■

What this theorem is saying is that if we want to compute the GCD of three numbers, we simply compute the GCD of the first two, and then the GCD of that number with the third. And although we have come up defintions and explanations for how to find a GCD, we do not yet have a foolproof way for computing one that does not involve a factor tree. So now we will state another method by which we can find a GCD that, while similar in spirit to a factor tree, is more formalized.

Definition- If $a = p_1^{\alpha_1} * p_2^{\alpha_2} * ..... * p_n^{\alpha_n}$, and $b = p_1^{\beta_1} * p_2^{\beta_2} * ..... * p_n^{\beta_n}$, then $(a,b) = p_1^{min(\alpha_1,\beta_1)} * p_2^{min(\alpha_2,\beta_2)} * ..... * p_n^{min(\alpha_n,\beta_n)}$

If this is confusing, some examples should clear it up:

ex: Looking at our old example (56, 462)=
$56 = 2^3 * 7^1$
$462 = 2^1 * 3^1 * 7^1 * 11^1$
Now, we apply our new definition: $(56, 462) = 2^{min(1,3)} * 3^{min(0,1)} * 7^{min(1,1)} * 11^{min(0,1)} = 2^1 * 3^0 * 7^1 * 11^0 = 14$ This is exactly what we got as a solution earlier.

The only question about this definition might be what the function *min* means. If it isn't self-evident, the *min* function simply chooses the smaller of the numbers in the parenthasis. So $min(12,17) = 12$, while $min(5,5) = 5$.

Definition- The **LEAST COMMON MULTIPLE (LCM)** of integers a and b, $[\mathbf{a},\mathbf{b}]$, is the smallest integer that is divisible by both a and b.

ex: [6,8]=24
ex: [11,5]=1
ex: [16,28]=112

Nothing too difficult here, but we don't yet have a great way to compute these values. Let's start with the alternate definition:

<u>Definition</u>- If $a = p_1^{\alpha_1} * p_2^{\alpha_2} * ..... * p_n^{\alpha_n}$, and $b = p_1^{\beta_1} * p_2^{\beta_2} * ..... * p_n^{\beta_n}$, then $[a, b] = p_1^{max(\alpha_1,\beta_1)} * p_2^{max(\alpha_2,\beta_2)} * ..... * p_n^{max(\alpha_n,\beta_n)}$

It looks a lot like the definition for GCD, for reasons that will become clear shortly. And the *max* function operates opposite of the *min* function, taking the larger of the numbers inside the parenthasis. We will save examples for the exercises at the end of the section.

<u>THEOREM (4.2.7)</u>- $a, b \in \mathbb{Z}^+ \longrightarrow ab = (a, b)[a, b]$
<u>Proof</u>- We know that, by the FTOA, that $a = p_1^{\alpha_1} * p_2^{\alpha_2} * ..... * p_n^{\alpha_n}$, and $b = p_1^{\beta_1} * p_2^{\beta_2} * ..... * p_n^{\beta_n}$, where some of the alphas and betas may be equal to 0. Then we know that $(a, b)[a, b] = p_1^{min(\alpha_1,\beta_1)} * p_2^{min(\alpha_2,\beta_2)} * ..... * p_n^{min(\alpha_n,\beta_n)} * p_1^{max(\alpha_1,\beta_1)} * p_2^{max(\alpha_2,\beta_2)} * ..... * p_n^{max(\alpha_n,\beta_n)}$. Now if we rearrange the terms, we get $p_1^{min(\alpha_1,\beta_1)} * p_1^{max(\alpha_1,\beta_1)} * ..... * p_n^{\min(\alpha_1,\beta_1)} * p_n^{max(\alpha_n,\beta_n)}$ We can combine terms with the same base to get $p_1^{min(\alpha_1,\beta_1)+max(\alpha_1,\beta_1)} * ..... * p_n^{min(\alpha_n,\beta_n)+max(\alpha_n,\beta_n)}$. But that is equal to $p_1^{\alpha_1+\beta_1} * ..... * p_n^{\alpha_n+\beta_n}$. (We reserve the reason why for a question in the exercises.) Separate the bases to yield $p_1^{\alpha_1} * p_1^{\beta_1} * ..... * p_n^{\alpha_n} * p_n^{\beta_n} = p_1^{\alpha_1} * ..... * p_n^{\alpha_n} * p_1^{\beta_n} * ..... * p_n^{\beta_n} = ab$.

Q.E.D.

So now we have a way of computing LCM with relative ease. We simply find the product ab, and divide by (a, b)!

<u>Exercises</u>

1. Are the following numbers prime or composite? How can you tell without using any theorems?

   (a) 43

   (b) 57

   (c) 91

   (d) 301

   (e) 507

2. Apply the fundamental theorem of arithmetic to each of the following integers:

(a) 72

(b) 5005

(c) 7897

(d) 100001

3. Use the contrapositive theorem to determine whether or not the numbers in question 1 are prime.

4. Prove that Goldbach's Conjecture holds for the following numbers:

   (a) 24

   (b) 50

   (c) 500

5. Assume the truth of Goldbach's Conjecture and use it to prove that any odd number greater than 5 can be written as the sum of three prime numbers.

6. Compute the following values:

   (a) (9,144)

   (b) (125,1125)

   (c) (210,858)

   (d) (9888,6060)

7. Prove by induction that $(a, b, c, ..., n) = (((a, b), c)), d, ...n)$

8. Find the Least Common Multiple of the following pairs of numbers:

   (a) $[7, 8]$

   (b) $[9, 24]$

   (c) $[12, 48]$

   (d) $[210, 858]$

   (e) $[9888, 6060]$

9. Compute (999,1000)

10. Compute (9998,10001)

11. Find the GCD: $(3x, 6x^2 + 15x + 1)$

12. Find all pairs of integers a and b that have a GCD of 18 and an LCM of 540.

13. Why is $p_1^{min(\alpha_1,\beta_1)+max(\alpha_1,\beta_1)} * ..... * p_n^{min(\alpha_n,\beta_n)+max(\alpha_n,\beta_n)} = p_1^{\alpha_1+\beta_1} * ..... * p_n^{\alpha_n+\beta_n}$?

(4.3) – Linear Diophantine Equations

In the last section, we defined the GCD, and figured out how to compute it by using the Fundamental Theorem of Arithmetic. The numeric examples we tried it on all worked nicely, but a question arises- how do we compute the GCD of numbers too large to break into "easy" primes? For example, if we were asked to compute (13125,896), is it easy to use the techniques from section 4.2? Maybe, maybe not. Regardless, you will eventually come across numbers that are too unwieldy to manipulate without a calculator. That's when we have to come up with a new technique. But before we attempt that, we want to prove a few things first.

THEOREM (4.3.1)- If $a, b \in \mathbb{Z}$, and $(a, b) = d \longrightarrow (\frac{a}{d}, \frac{b}{d}) = 1$
Proof- Say $(\frac{a}{d}, \frac{b}{d}) = n$. Then $n|\frac{a}{d}$ and $n|\frac{b}{d} \to nk = \frac{a}{d}$ and $nl = \frac{b}{d} \to nkd = a, nld = b \to (nd)k = a, (nd)l = b$. So, nd is a common factor of both a and b, which means that $nd|(a, b) = d$. But if $nd|d \to n = 1$. Can you figure out why that is? Therefore, $(\frac{a}{d}, \frac{b}{d}) = 1$

Q.E.D.

Okay, so that's well and good, but we might not have much of an idea what this theorem is saying. Put plainly, what it's saying is that if we take two integers, and divide out ALL that they have in common, the only intger that they have left in common is 1. This may seem like a pointless theorem (don't they all?) but you will soon see that it is going to help us build a very important mathematical process. The following theorem serves the same function.

THEOREM (4.3.2)- If $a, b, c \in \mathbb{Z} \longrightarrow (a + bc, b) = (a, b)$
Proof- We will prove this via a double inclusion. Say that R is the set of all factors of both $a + bc$ and b and say S is the set of all factors of both a and b.
$\Longleftarrow$Let's say that n is a common factor of a and b. Then $n|a, n|b \to n|bc$ (Why?) $\to n|(a{+}bc)$ So n is a factor of both a and $a{+}bc$, and thus a member of set $R \to S \subseteq R$.
$\Longrightarrow$. Now say m is a factor of both $a + bc$ and $b \to m|(a + bc), m|b$. So $m|bc \to m|a$ (Why?). Now, since m is a factor of both a and b, $R \subseteq S$.

■

This may seem like an arbitrary thing to prove, but it most certainly is not. Take a close look and you might see that $a + bc$ bears a resemblance to the equation used in the division algorithm. This is no coincidence, obviously. This theorem is part of the basis for the main thrust of this chapter. We can illustrate this with a simple question:

ex: Without use of a calculator, find the value of (13125,896)
Er..... this one may not be so easy. Sure, we could break both numbers down using the FTOA, but without a calculator, the division may prove difficult. So what do we do? Believe it or not, we can combine our theorem 4.3.2 with the division algorithm to form a technique that will knock off just this type of question! Since this is the first time we will attempt this technique, every step will be explained. We will not adhere to this level of thoroughness in the future.

$$13125 = 14(896) + 581 \tag{1}$$

This is our first application of the division algorithm, using the two numbers in question. But how does this relate to our earlier theorem? We can say that $13125 = a + bc, 14 = c, 896 = b, a = 581$. We know that $(a + bc, b) = (a, b)$, so our goal should be to use the numbers a and b to find a greatest common divisor. So.....

$$896 = 1(581) + 315 \tag{2}$$

In this case, $896 = a_2 + b_2c_2, 1 = c_2, 581 = b_2, 315 = a_2$. From here, we will iterate, using the division algorithm on each new a_k and b_k. This is how it looks:

$$581 = 1(315) + 266 \tag{3}$$

$$315 = 1(266) + 49 \tag{4}$$

$$266 = 5(49) + 21 \tag{5}$$

$$49 = 2(21) + 7 \tag{6}$$

$$21 = 3(7) + 0 \tag{7}$$

The GCD is equal to the last nonzero remainder in our iterated division algorithms. So, as a quick answer, $(13125, 896) = 7$. But let's take a closer look at EXACTLY what our theorem was saying as it pertains to this particular example. It said that (13125,896)=(896,581)=(581,315)=(315,266)=(266,49)=(49,21)=(21,7)=7. Without our theorem, we would not be able to make this claim. Now, the process that we just used has a name, and it is called the **EUCLIDEAN ALGORITHM**.

ex: (6669,1485) We will apply the Euclidean Algorithm to find a solution:
6669=4(1485)+729
1485=2(729)+27
729=27(27)+0
So, (6669,1485)=27

We now have techniques by which we can find the GCD (without a calculator) given *any* two integers. This is incredibly useful for many reasons, one of which is that it can help us solve real-life questions. Take this question for example: "Oranges cost 6 cents apiece, and apples cost 11 cents apiece. If a man spends \$3.45 to purchase some of each fruit, how many of each did he buy?" Up until this point, you would probably have tackled this question by trial and error. You may have noticed that we are looking for integer answers, because you cannot (in most stores) buy half of an apple, or a tenth of an orange. Armed with that information, you might've plugged in values for the presumed number of apples, and then tried to figure out if the number of oranges ended up as an integers. This process might get you an answer, but it is time consuming, and, of course, not very effective when the numbers get large. This is where the Euclidian Algorithm comes in.

Often for real-life questions, we need to find integer solutions. The question above is one such example. Another might be if you wanted to figure out how many students take Discrete Math and how many take Calculus. You can't have a fraction of a student! Questions in which the solution must be an integer are called **LINEAR DIOPHANTINE EQUATIONS**, or LDEs. For the remainder of this section, we will deal with this type of equation. Look at the following equations, and see if you can find integer solutions:

1. $2x + 4y = 3$

2. $2x + 4y = 6$

3. $6x + 15y = 93$

4. $8x + 28y = 122$

My guess is that you were able to get (1) and (2) pretty easily, but had a bit more trouble determining whether or not (3) and (4) were true. Obviously this is not a guess-and-check question; it uses the techniques we have developed over the course of this section.

1. This equation has no integer solutions for x and y. You can see this if you notice that both $2x$ and $4y$ are even, so they cannot add to an odd.

2. This equation has a pretty apparent solution for x and y. One possible solution would be $x = 1, y = 1$, but that is not the only solution.

3. This one is a bit more difficult than the others, but if we try hard enough, we can come up with $x = 8, y = 3$. Again, this is not the only solution.

4. There is no obvious way (yet) to determine whether or not there are solutions for this one. It turns out that you can try for as long as you like, and you will not be able to find integers that satisfy x and y for this equation.

$\star$ And now to reveal the magic behind the trick: If $(a, b)|c$, we can find integers x and y s.t. $ax + by = c$, which is a solution to an LDE. Better yet, we can find x, y s.t. $ax + by = cd$. Let's translate that for the purposes of these questions:

1. $(2, 4) = 2 \nmid 3 \rightarrow$ No solution.

2. $(2, 4) = 2|6 \rightarrow$ We can find solutions.

3. $(6, 15) = 3|93 \rightarrow$ Solutions exist.

4. $(8, 28) = 4 \nmid 122 \rightarrow$ No solution.

$\star$ So we have been saying that we can find solution**s**, as in plural. This is because if $(a, b)|c$, there are an **infinite** number of solutions to the linear diophantine equation $ax + by = c$. We have already stated that if $(a, b) \nmid c$, then there are no solutions. So for a generic linear diophantine equation, there are only two possibilities for the number of solutions- none or infinite.

ex: Find x, y that fulfill the LDE $2x + 8y = 100$.
Well, we immediately see that $(2, 8) = 2|100$, so there are an infinite number of solutions. By inspection, we can easily find $x = 10, y = 10$ as a single solution of the equation.

ex: Find an x, y that fullfills the LDE $14x + 77y = 623$.
This one is way more difficult than the previous example, and trial and error probably won't cut it as a viable technique. The first thing we can check is whether or not there are even solutions. $(14, 77) = 7|623$ tells us there are an infinite number of them. We need to find one. This is how we can use the Euclidean Algorithm to do this:
77=5(14)+7 $\longrightarrow$ 14=2(7)+0
We will now perform algebra on the first equation to solve for the GCD, which is 7:
77=5(14)+7 $\longrightarrow$ 7=77-5(14) Now, a simple calculation tells us that 7(89)=623, so we can multiply both sides of the equation by 89 to get 89(7)=89(77)-445(14). Note that our final equation is of the form $14x + 77y = 623$. We found a solution- $x = -445$ and $y = 89$.

Here is the precise process that we are using to solve a LDE $ax + by = c$ for x and y: First we find $(a, b) = d$. If $d|c$, then we can find a solution. If $d \nmid c$, there are no solutions. We use the Euclidean Algorithm to find d, even if we can figure it out using simpler techniques. We reverse the Euclidean Algorithm until we have the GCD written as a linear combination of its components. Finally, we multiply through by $\frac{c}{d}$ on both sides of the equation to solve for our x and y.

The difficulty of this process comes in reversing the Euclidian Algorithm. In the previous example, it was simple because we only had one equation to deal with. This is not always the case, as you will see in the next example.

ex: Find x, y in the LDE $49x + 20y = 94$
We start with the Euclidean Algorithm, and then reverse it.
$49 = 2(20) + 9 \rightarrow 20 = 2(9) + 2 \rightarrow 9 = 4(2) + 1$
We will be a bit more careful in the process of solving for the GCD, which is 1:
1=9-4(2)
1=9-4[20-2(9)]
1=9-4(20)+8(9)
1=9(9)-4(20)
1=9[49-2(20)]-4(20)
1=9(49)-18(20)-4(20)
1=9(49)-22(20)
We now have the GCD (1) written as a linear combination of 49 and 20, which is what we wanted. Now we wimply multiply through by 94, giving us:
94=(9*94)(49)-(22*94)(20) $\longrightarrow$ 94=846(49)-2068(20). So $x = 846$ and $y = -2068$.

Remember that we are finding but ONE solution to the linear diophantine equation, and there is no guarantee that this is the simplest solution. As a matter of fact, this technique will almost always guarantee us a solution than many others. Our next step should be to figure out how to find ALL possible solutions to a linear diophantine equation. Luckily, we have a theorem (one we will not prove) for this kind of question.

THEOREM (4.3.3)- Let $a, b \in \mathbb{Z}$, with $d = (a, b)$. The equation $ax + by = c$ has no integral solution if $d \nmid c$. If $d|c$, then there are infinitely many integral solutions. Moreover, if $x = x_0, y = y_0$ is a particular solution to the equation, then all solutions are given by: $x = x_0 + \frac{b}{d}n$ and $y = y_0 - \frac{a}{d}n$.

Before explaining the theorem, we want to note that you can divide out d in the begining so that the GCD is equal to 1. This will make the subsequent formulae much easier to deal with. There may be questions about what n is, and the simplest answer is that it is a variable. We do not solve for n; as a matter of fact, once we have plugged in for a, b, d, x_0, y_0, the only remaining variable is n. Whatever number you choose to plug in for n will yield a valid solution. Now, what this theorem is basically saying is that if you can find an **initial solution** to the LDE, then you can use the formula to find ALL solutions. Let's look at a somewhat more complicated example to illustrate this concept.

ex: How many different ways are there to make \$510 out of twenty and fifty dollar bills?

The first thing we want to do is set this up as an LDE. That's easy enough- $20x+50y = 510$. We can divide out our $d = 10$ from both sides to get $2x + 5y = 51$. Now we reverse the Euclidean Algorithm to write the GCD as a linear combination of its components: $5 = 2(2) + 1 \rightarrow 1 = 5 - 2(2)$. Now we multiply both sides by 51 to get $51 = 51(5) - 102(2)$. According to Theorem 4.3.3, we need to find a single solution to our LDE, and that solution is $x_0 = -102, y_0 = 51$. If we wanted to find ALL possible solutions to the LDE, we would simply plug into the given formula to get: $x = -102+5n$ and $y = 51-2n$. These two equations represent ALL possible solutions to the LDE. No matter what number you plug in for n, you will get a solution to the original LDE that works. However, we are dealing with a situation where negative values are not possible. The reason for this should be obvious- you cannot have a negative number of fifty or twenty dollar bills. So we are only looking for positive values for x and y. We can find these possible values by applying simple algebra to the equations $x \geq 0$ and $y \geq 0$.
$-102 + 5n \geq 0 \rightarrow 5n \geq 102 \rightarrow n \geq 20.4$
$51 - 2n \geq 0 \rightarrow 51 \geq 2n \rightarrow 25.5 \geq n$
Combining those two equations gives us $20.4 \leq n \leq 25.5$, which gives us integer values for $n = 21, 22, 23, 24, 25$. Plugging those values back into our equations gives us solutions $(3, 9), (8, 7), (13, 5), (18, 3), (23, 1)$.
These solutions should make sense- 3 twenty dollar bills and 9 fifty dollar bills give you \$510. The other solutions work as well.

Exercises

1. Answer the question posed in the first theorem of the section.

2. Theorem (4.3.2), at one point, asks the question "Can you figure out why that is?" If you can, explain it.

3. Use the Euclidean Algorithm to find the GCD of the following pairs:

   (a) (32,26)

   (b) (414,662)

   (c) (750,124)

4. Find a single solution for each of the following Linear Diophantine Equations:

   (a) $3x + 4y = 17$

   (b) $12a + 18b = 50$

(c) $25x + 95y = 970$

5. Find ALL possible solutions to the LDEs in the previous question.

6. Find all possible solutions to the following LDEs.

   (a) $30x + 47y = -11$

   (b) $102x + 1001y = 1$

7. A shopper spends a total of \$5.49 for fruit made up of apples, which are 18 cents each, and oranges, which are 33 cents each. What is the minimum pieces of fruit she could have bought?

8. Is it possible to have 50 coins, all of which are pennies, dimes, or quarters, with a total worth three dollars?

9. Find all integer solutions of the following systems of linear diophantine equations:

   (a) $x + y + z = 100, x + 8y + 50z = 156$

   (b) $x + y + z = 100, x + 6y + 21z = 121$

   (c) $x + y + z + w = 100, x + 2y + 3z + 4w = 300, x + 4y + 9z = 16w = 1000$

By this point, you should be an expert at dealing with prime factorizations, GCDs and LCMs. We have broken down many properties of division that you may have taken for granted, and worked extensively with the manipulation of integers. In this section, we further explore the various properties of division by introducing the concept of of a *congruence*. The concept of a congruence is one that is prevalent in almost every single branch of mathematics, and one that should not be taken lightly. One of the simpler congruences you will encounter in your math life is the one involving.....

(4.4) – Modular Arithmetic

Definition- $m \in \mathbb{Z}^+, a, b \in \mathbb{Z}$. We say $\boldsymbol{a}$ **IS CONGRUENT TO** $\boldsymbol{b}$**(mod** $\boldsymbol{m}$**)**, $\mathbf{a \equiv b}$**(mod** m**)**, if $m|(a-b)$.

The notation $\equiv$ simply indicates that two integers a, b are congruent (mod whatever), or *equivalent* (mod whatever). Its meaning is given above. One thing that may still be confusing is why exactly we have that (mod) thing up there. Mod is shorthand for *modulus*, or the number that we are dividing by. We will say more about the modulus after the following examples.

ex: $23 \equiv 2(\text{mod } 7)$ This is a true statement because $7|(23-2)$.
ex: $25 \not\equiv 3(\text{mod } 8)$ This is not true because $8 \nmid (25-3)$
ex: $28 \equiv -8(\text{mod } 9)$ Can you figure out why?

Those three examples highlight one way that we can prove whether or not two integers are congruent. This is not the only way, however. An alternate way to look at the definition of $a \equiv b(\text{mod } m)$ is to say that if a and b are equivalent (mod m), then they yield the same remainder when divided by m. This is probably a more natural definition than the one given earlier, but circumstance will dictate when you will use which definition.

If we look back at the three examples, we can apply this alternate definition to good effect. For the first one, we can note that both 23 and 2 give a remainder of 2 when divided by 7. In the second example, this is not the case. 8 goes into 3 zero times with a remainder of three, while 8 goes into 25 three times with a remainder of 1. So the two numbers are not congruent (mod 8).

And important thing to internalize is this: Just because two numbers are cogruent (mod m), it does not mean they are equal. A congruence is a binary relationship, or a relationship between two mathematical things. You've seen binary relationships before, notably equalities and inequalities. A congruence between two numbers is a weaker relationship than an equality, but possesses desirable properties nonetheless. One of those properties is the following:

$\star$ If two integers are congruent (mod m), then you can replace one with the other and the eqivalence will still be valid.

ex: $8+2 \equiv 3+2 (\text{mod } 5)$ The 8 can be replaced with a 3 without penalty because both give the same remainder when divided by 5.

THEOREM (4.4.1)- If $a, b \in \mathbb{Z}$, then $a \equiv b (\text{mod } m) \iff \exists k$ s.t. $a = b + km$
Proof- This is two-way proof:
$\implies a \equiv b(\text{mod } m) \to m|(a-b) \to mk = a - b \to a = b + km$
$\impliedby a = b + km \to a - b = km \to m|(a-b) \to a \equiv b(\text{mod } m)$

■

Nothing terribly heavy here, and you'll notice that each half of the proof is the direct reverse of the other half. This theorem shows the intimate connection between congruences over a modulus and the divisibility theorems we proved in section 4.2. Perhaps it was an indicator when we brought up the concept of a remainder, but modular congruences are just another way of expressing division. Look at it this way:

ex: $97 \equiv -2(\text{mod } 33) \to 97 = -2 + 3(33)$

We have mentioned the fact that any two congruent integers can replace one another in a modular equivalence. We will formalize this concept with another definition.

Defintition- We can split all integers into m sets that we call **CONGRUENCE CLASSES (mod m)**. Each class is mutually congruent (mod m), and includes only numbers that give the same remainder as other elements in the class. Every single integer belongs to one and only one congruence class.

This is a complicated way of saying that every single number gives you a remainder when divided by m, and no number gives two remainders. Of course, we have known this since we started working with the division algorithm in section 4.2. As a reminder, we can replace any number in an equivalence with any other number in its congruence class. Now, since this is a new concept, it might still seem a little slippery. For example, how many congruence classes are there? That's a question that can only be answered given a particular modulus. As a matter of fact, the number of congruence classes (mod m) is precisely m. The reason for this is simple- given any divisor m, there are m possible remainders: 0,1,2,.....,$m-2, m-1$.

Let's look at the Equivalence (congruence) classes (mod 5):
.....,-10,-5,0,5,10,.....
.....,-9,-4,1,6,11,.....
.....,-8,-3,2,7,12,.....
.....,-7,-2,3,8,13,.....
.....,-6,-1,4,9,14,.....

As you can see, every single integer belongs to one of the five congruence classes, and no integer belongs to more than one. Furthermore, given a particular congruence class, ever single element within yields the same remainder when divided by 5. All that is left is to figure out is what we should call each of the classes. As a matter of convention, each class is named after the remainder when any element is divided by the modulus. In the above example, the congruence classes are $\{0, 1, 2, 3, 4\}$. From here on out, we will refer to the remainder as the **LEAST NON-NEGATIVE RESIDUE** of a particular modulus. When solving equivalences for a variable, we will ALWAYS write our solution as a least non-negative residue. Better get used to that!

ex: To what congruence class does 400(mod 7) belong? 7 goes into 400 57 times, with a remainder of 1, so the least non-negative residue for 400 is 1(mod 7).
ex: How about -400(mod 7)? Be careful! The answer is not 1(mod 7). This question is more difficult because most students are unaccustomed to dividing into negative numbers. How many times does 7 go into -400? You might be tempted to say -57, but that would yield the following division algorithm statement: $-400 = 7(-57) - 1$. Note that the remainder in this case is -1, which is not allowed in the division algorithm. So, it turns out that we actually want $-400 = 7(-58) + 6$, and the remainder is 6. So $-400 \equiv 6(\text{mod } 7)$.

Now, there are ways to circumvent dividing by negative numbers, but they require a little bit more information about the nature of modular congruences.

THEOREM 4.4.2- $a, b, c \in \mathbb{Z}, m \in \mathbb{Z}^+$ s.t. $a \equiv b(\text{mod } m)$. Then:

1. $a + c \equiv b + c(\text{mod } m)$

2. $a - c \equiv a - c (\text{mod } m)$

3. $ac \equiv bc (\text{mod } m)$

Proof- It should be fairly obvious what these theorems are trying to say, but plugging in numbers can make it even clearer. Now let's prove each separately:

1. $a \equiv b(\text{mod } m) \to m|(a-b) \to mk = a - b \to mk = a + c - c - b \to mk = (a+c) - (b+c) \to m|[(a+c) - (b+c)] \to a + c \equiv b + c(\text{mod } m)$

2. $a \equiv b(\text{mod } m) \to m|(a-b) \to mk = a - b \to mk = a - c + c - b \to mk = (a-c) - (b-c) \to m|[(a-c) - (b-c)] \to a - c \equiv b - c(\text{mod } m)$

3. $a \equiv b(\text{mod } m) \to m|(a-b) \to mk = a - b \to mkc = ac - bc \to m|(ac - bc) \to ac \equiv bc(\text{mod } m)$

Q.E.D.

This theorem states that the normal rules for addition, subtraction and multiplication hold in an equivalence. These examples show how this works:

ex: $12 \equiv 5(\text{mod } 7) \to 12 + 6 \equiv 5 + 6(\text{mod } 7) \to 18 \equiv 11(\text{mod } 7)$ Dividing each of those numbers by 7 shows that you get a remainder of 4, so the equivalence holds.
ex: $21 \equiv 5(\text{mod } 8) \to 21(47) \equiv 5(47)(\text{mod } 8) \to 987 \equiv 235(\text{mod } 8)$ Both numbers yield a remainder of 3 when divided by 8.

So now we have rules for three of the four main operators that are seen in math. That begs the question of whether or not the rules for division work the same in an equivalence as they do in an equality.

ex: $14 \equiv 6(\text{mod } 8) \to 14/2 \equiv 6/2(\text{mod } 8)$? NO! $7 \not\equiv 3(\text{mod } 8)$. And so we see that the rules of division do not work in the normal way. We have to tweak the rules just a bit to get it to work.

THEOREM (4.4.3)- $a, b, c \in \mathbb{Z}, m \in \mathbb{Z}^+$, and $d = (c, m), ac \equiv bc(\text{mod } m)$. Then $a \equiv b(\text{mod } \frac{m}{d})$

There's a lot going on in this statement, and it is much easier to see if you simply plug in numbers that fulfill the assumption. Before we prove it, we will try some examples that illustrate the idea of the theorem:

ex: $24 \equiv 45(\text{mod } 21) \to 8 * 3 \equiv 15 * 3(\text{mod } 21) \to 8 \equiv 15(\text{mod } 7)$ In this case, $a = 8, b = 15, c = 3$, and so $(c, m) = (3, 21) = 3 = d$.

ex: $50 \equiv 20 (\text{mod } 15) \rightarrow 10 * 5 \equiv 4 * 5 (\text{mod } 15) \rightarrow 10 \equiv 4 (\text{mod } 3)$. Now, note that (10,4)=2, and (2,3)=1, so $5 \equiv 2 (\text{mod } 3)$.

So there is a way to divide in modular arithmetic, but it can leave you with a modulus smaller than the one with which you began. Of course this is not always the case:

Corollary to (4.4.3)- $a, b, c \in \mathbb{Z}, m \in \mathbb{Z}^+, (c, m) = 1, ac \equiv bc (\text{mod } m)$. Then $a \equiv b (\text{mod } m)$

ex: $18 \equiv 33 (\text{mod } 5) \rightarrow 6 \equiv 11 (\text{mod } 5)$

We've shown some examples, but up to this point, we've omitted the proof of Theorem (4.4.3). Now we un-omit it.

Proof- $ac \equiv bc (\text{mod } m) \rightarrow m | (ac - bc) \rightarrow m | c(a - b) \rightarrow mk = c(a - b)$ Now take a slight detour to remember that $d = (c, m)$ and thus $d|c$ and $d|m$. So $\frac{mk}{d} = \frac{c}{d}(a + b) = \frac{m}{d}k$. Now go back and look up Theorem (4.3.1), which says $(m, c) = d \rightarrow (\frac{m}{d}, \frac{c}{d}) = 1$. So $\frac{m}{d} \nmid \frac{c}{d}$, and yet $\frac{m}{d} | \frac{c}{d}(a - b)$, which implies that $\frac{m}{d} | (a - b) \rightarrow a \equiv b (\text{mod } \frac{m}{d})$.

■

THEOREM (4.4.4)- $a, b, c, d \in \mathbb{Z}, m \in \mathbb{Z}^+$ and $a \equiv b (\text{mod } m), c \equiv d (\text{mod } m)$. Then the following are true:

1. $a + c \equiv b + d (\text{mod } m)$
2. $a - c \equiv b - d (\text{mod } m)$
3. $ac \equiv bd (\text{mod } m)$

This may look like Theorem (4.3.2), but if you try it with numbers you will see that this is not simple modular arithmetic. This theorem is telling us that we can add, subtract or multiply two different equivalences so long as the modulus is the same in both.

Proof- As before, we prove each separately:

1. $a \equiv b (\text{mod } m), c \equiv d (\text{mod } m) \rightarrow mk = (a - b), ml = (c - d)$. Now that we have two equations, we can simply add them together, giving us $mk + ml = (a - b) + (c - d) \rightarrow m(k - l) = (a + c) - (b + d) \rightarrow m | [(a + c) - (b + d)] \rightarrow a + c \equiv b + d (\text{mod } m)$.
2. $a \equiv b (\text{mod } m), c \equiv d (\text{mod } m) \rightarrow mk = (a - b), ml = (c - d) \rightarrow mk - ml = (a - b) - (c - d) \rightarrow m(k - l) = (a - c) - (b - d) \rightarrow m | [(a - c) - (b - d)] \rightarrow a - c \equiv b - d (\text{mod } m)$

3. $a \equiv b(\text{mod } m), c \equiv d(\text{mod } m) \rightarrow mk = (a-b), ml = (c-d)$. There are a few different ways you can take the proof from here, but we will attempt to be clever. $mkc = (ac - bc), mlb = cb - db \rightarrow mkc + mlb = ac - bc + bc - db \rightarrow m(kc + lb) = ac - db \rightarrow m|(ac - db) \rightarrow ac \equiv bd(\text{mod } m)$

Q.E.D.

ex: $13 \equiv 3(\text{mod } 10)$, $2 \equiv 22(\text{mod } 10)$ Then $13 + 2 \equiv 3 + 22(\text{mod } 10)$, $13 - 2 \equiv 3 - 22(\text{mod } 10)$, and $13 * 2 \equiv 3 * 22(\text{mod } 10)$

Exercises

1. Find the LNR of each of the following:
   (a) 22(mod 15)
   (b) 50(mod 7)
   (c) -8(mod 9)
   (d) 3(mod 4)
2. Find the LNR of each:
   (a) 1000(mod 35)
   (b) -234(mod 41)
   (c) 14^5(mod 13)
3. Find the least non-negative residue for each of the following:
   (a) $1 + 2 + 3 + ... + 18(\text{mod } 19)$
   (b) $20 + 21 + 22 + ... + 192(\text{mod } 19)$
4. True or false:
   (a) $77 \equiv -12(\text{mod } 5)$
   (b) $9 \equiv -9(\text{mod } 5)$
   (c) $100 \equiv 200(\text{mod } 15)$
   (d) $1600 \equiv 269(\text{mod } 11)$
5. For which positive integers m is each of the following true?
   (a) $27 \equiv 5(\text{mod } m)$

(b) $1000 \equiv 1 (\text{mod } m)$

(c) $1331 \equiv 0 (\text{mod } m)$

6. Prove that every integer $m \equiv 0 (\text{mod } 1)$

7. What property of integers does (mod 2) test?

8. What is the LNR of x in each of the following?

   (a) $10! \equiv x (\text{mod } 400)$

   (b) $11 \equiv 3 (\text{mod } x)$

   (c) $1! + 2! + 3! + ... + 100! (\text{mod } 2)$

   (d) $1! + 2! + 3! + ... + 100! (\text{mod } 7)$

   Show that if $c > 0, m > 0$ and $a \equiv b (\text{mod } m)$, then $ac \equiv bc (\text{mod } mc)$.

9. If $(x, 3) = 1$, and $(y, 3) = 1$, show that $(x^2 + y^2, 3) = 1$.

10. Show that if n is odd, then $1 + 2 + 3 + ... + n \equiv 0 (\text{mod } n)$. If n is even, solve for x in terms of n: $1 + 2 + 3 + ... + n \equiv x (\text{mod } n)$.

11. Prove by induction: $4^n \equiv 1 + 3n (\text{mod } 9)$

12. Prove the corollary to Theorem (4.4.3)

So we learned a whole new way of looking at division in the previous section, but the question remains- why did we bother? It turns out that modular arithmetic has a slew of uses beyond simple division. In this section we will advance our discussion of modular arithmetic and discover some of these uses. Let's start with a theorem that may not seem to serve any purpose, but is pretty interesting nonetheless.

(4.5) – Mods are Useful!

THEOREM (4.5.1)- If p is a prime number greater than or equal to 5 $\longrightarrow p^2 \equiv 1 (\text{mod } 24)$

Proof- This probably seems pretty random to you, and I agree that it is. But just take any prime greater than 3- 7 for example. Well, $7^2 = 49 \equiv 1(\text{mod } 24)$. It's weird, but now that we have a basic grasp of mods, we can easily prove this.

Let's take any prime, square it and assume that it is congruent to 1(mod 24). $p^2 \equiv 1(\text{mod } 24) \rightarrow p^2 - 1 \equiv 0(\text{mod } 24) \rightarrow 24|(p^2 - 1) \rightarrow 24|(p-1)(p+1)$. Here is where a little analysis will come in handy. We will only look at the right side of the division sign. First notice that since $p \geq 5$, then p is odd, and thus $p-1, p+1$ are even numbers. Better yet, they are two consecutive even numbers. We know from section 4.1 that given any two consecutive even integers, one of them will be divisible by 2 and the other will be divisible by 4. That means that the product of the two of them must be divisible by 8.

Now here comes the tricky part- look at the three consecutive numbers $p-1, p, p+1$. Since they are three consecutive numbers, one of them must be divisible by 3. But p cannot be divisible by 3 because it is a prime number. This means that either $p-1$ or $p+1$ is divisible by 3. So let's review what we have here: the product $(p-1)(p+1)$ is divisible by 8, and one of either $p-1$ or $p+1$ is divisible by 3. Overall that tells us the product $(p-1)(p+1) = p^2 - 1$ is divisible by 24. And $24|(p^2 - 1) \rightarrow p^2 \equiv 1(\text{mod } 24)$

Q.E.D.

THEOREM (4.5.2)- If a number is divisible by 9, the sum of the digits of that number is divisible by 9

Proof- Yes, we proved this earlier, but look at how a modular argument makes quick work of it. We will work with a four-digit number for convenience, but you can prove this for an arbitrary number of digits. Remember expanded form? We can write a typical four-digit number as $1000a + 100b + 10c + d$. Now, let's reduce that entire equation (mod 9) b dividing each term by 9 and finding the remainder of each. This gives us $a + b + c + d (\text{mod } 9)$. But wait..... that's EXACTLY what we wanted to prove.

■

So you have now seen a little bit of the flexibility we gain by applying the rules of modular arithmetic. It can be used to make more difficult proofs easier, or to prove interesting facts that you might never have thought of before. Now we will prove something that will further aid us in our journey to NEVER use a calculator again. (Note: sometimes you will have to use a calculator)

THEOREM (4.5.3)- If $a, b \in \mathbb{Z}, k, m \in \mathbb{Z}^+$ and $a \equiv b (\text{mod } m) \longrightarrow a^k \equiv b^k (\text{mod } m)$

Proof- This one will fall really easily if we just remember a simple algebraic fact. Before stating this fact, we will show a few examples of how it works:

$a^1 - b^1 = a - b$

$a^2 - b^2 = (a - b)(a + b)$

$a^3 - b^3 = (a - b)(a^2 + ab + b^2)$

$a^4 - b^4 = (a - b)(a^3 + a^2b + ab^2 + b^3)$

$a^5 - b^5 = (a - b)(a^4 + a^3b + a^2b^2 + ab^3 + b^4)$

$a^k - b^k = (a - b)(a^{k-1} + a^{k-2}b + ... + ab^{k-2} + b^{k-1})$

So there it is- $(a-b)$ always divides $a^k - b^k$. And here's the complete proof- $a \equiv b (\text{mod } m) \to m|(a - b)|(a^k - b^k) \to m|(a^k - b^k) \to a^k \equiv b^k (\text{mod } m)$.

Q.E.D.

The use of this theorem may not be immediately clear. You probably understand that the theorem is saying that the process of exponentiation holds over an equivalence. Why we would care about this is yet a mystery. We know from the previous section that we can replace an integer (mod m) with any other integer in its congruence class. But what if we wanted to find the least non-negative residue of a REALLY large number. Look at the following:

ex: Find the least non-negative residue for each of the following:

(1) $2^{102} (\text{mod } 31)$

(2) $3^{83} (\text{mod } 241)$

1. $2^{102} \equiv (2^6)^{17} \to 32^{17} \equiv 1^{17} \equiv 1 (\text{mod } 31)$ Now, where did we use the theorem? When we replaced 32^{17} with 1^{17}. Of course, 1 raised to any power is simply 1, and thus the question is easy to complete.

2. $3^{83} \equiv (3^5)^{16} * 3^3 \rightarrow 243^{16} * 3^3 \rightarrow 2^{16} * 3^3 \equiv (2^8)^2 * 27 \rightarrow 256^2 * 27 \equiv 15^2 * 27 \rightarrow 225 * 27 \equiv -16 * 27 \equiv -432 \equiv 50 (\text{mod } 241)$

Ok, so the second one wasn't easy at all. But here is the general process we use to reduce large numbers (mod m): We try to raise the base to a power that brings the value *close* to the modulus or a multiple of the modulus. Then we replace the base with its least non-negative residue. This number will be much smaler and much more managable than the original number. We then perform arithmetic and repeat the process until we get a number between 0 and the modulus, inclusive. Of course, none of that necessarily makes any sense to you. That's why it's important to try the exercises at the end of the section to gain mastery over this concept.

We will use this exponentiation theorem again in a moment, but first I would like to put it into context with a simple question:

Q: What is the last digit of 3^{2111}?
A: You might have some idea of how to do this one. Perhaps you know that $3^1 = 3, 3^2 = 9, 3^3 = 27, 3^4 = 81, 3^5 = 243, 3^6 = 729$...... If you keep going, you will see that the final digit follows the pattern of 3,9,7,1,3,9,7,1...... There are four different numbers in the pattern, so simply divide 2111 and find the remainder. Since the remainder is 3, the final digit is 7.

This is probably how you would have solved this question if you were asked it in high school or on the SATs. However, we know that a modulus keeps track of mathematical objects that repeat in a pattern, so we should try to apply some sort of modular arithmetic.

The first thing you might want to notice is what it means to find the least non-negative residue of a number (mod 10). Take a random number, like 4078, and find its LNR (mod 10). This is the same as finding the remainder when 4078 is divided by 10. A simple calculation shows that the remainder is 8. Try it for another number, like 56739. The remainder is 9. How about 14? The remainder is 4. You should notice by now that the LNR of any number (mod 10) is equal to the number's final digit. The reason is simple- all math that we have done up to this point has been done in base 10. So.....

$\star$ In order to find the final n digits of any integer x, find the least non-negative residue of $x (\text{mod } 10^n)$

Now let's retry the previous question- what is the last digit of 3^{2111}? Well now we know that all we have to do is solve for x in the equivalence $x \equiv 3^{2111} (\text{mod } 10)$. So $x \equiv 3^{2111} \equiv (3^2)^{1055} * 3^1 = 9^{1055} * 3 \equiv (-1)^{1055} 3 = -1 * 3 = -3 \equiv 7 (\text{mod } 10)$

Note how we get the same answer, which is obviously what we'd expect. Now this way may seem more difficult, but it is essential for the following question:

ex: What are the last two digits of 7^{1053}?
Because we want the last two digits, we will find the LNR of 7^{1053}(mod 100)
$7^{1053} \equiv (7^4)^{263} * 7^1 = 2401^{263} * 7 \equiv 1^{263} * 7 = 1 * 7 = 7$(mod 100) So the last two digits of 7^{1053} are 07.

So we've discovered yet another use for modular arithmetic. But perhaps we would like to expand from arithmetic to algebra, and see if the known rules apply to equivalences. In order to explore this concept, we introduce the *Cayley Table*, which is a way to display the relationship between elements in a set in a closed form. Here is an example of a Cayley Talbe for addition (mod 4):

+, (mod4)	**0**	**1**	**2**	**3**
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

The way we determine the value of a particular entry in the table is by selecting a box, adding the column header of the box to the row header of the box and then finding the LNR of the resulting number. For example, in the bottom right hand corner we have the number 2. This is found by adding 3 and 3 to get 6, and then reducing it (mod 4). Now, remember that every single integer is a member of some congruence class that is named by its least non-negative residue. This table keeps track of all integers, so long as we think of an integer as its representative congruence class.

There are few very important things you may wish to note about this particular table. The first is that the integers under addition (mod 4) are closed. If you remember back from chapter 1, this means that if you apply the operation (in this case, addition) to any two elements in the set, the result will also be an element of the set. This fact is the main reason why we can express the "universe" of addition (mod 4) in table form. Another fact of importance is the fact that 0 appears on every single line of the table. Why is this so important? Again, go back to chapter 1, and recall the concept of an identity, or an element that when applied to a member of a set, gives back that same member. The identity element of this set is 0 because $0 + k$ always results in k. The fact that the identity appears on every line tells us something very imporant- that every single element in this set has an inverse. Reviewing our earlier definition of inverse should help make sense of this concept. Inverses are a necessity if we wish to complete algebraic manipluations of elements in any set. We will return to this idea shortly. For now, let's do another table.

$*, (\text{mod} 5)$	**0**	**1**	**2**	**3**	**4**
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

The value of each box is found in the same way as in the previous table. As an example, $3 * 2 = 6 \equiv 1(\text{mod } 5)$. You should also recognize that if we ignore the strange case of 0, we see that each number in the set (representing all possible LNRs) is on every line. This also occured in our previous example. Let's get a little strict about computing the identity and inverses.

We will start by determining the identity, which must be unique to the set. The definition tells that for any element k, there exists an identity element e s.t. $k*e = k$. Since the identity element is unique, we can take any element and find out what maps k back to k. Let's choose 3 as our element. The identity definition would have us solve for e in the equation $3 * e = 3$. That's easy enough to solve even without a table- the solution is 1. But since we do have a table, let's use it. We simply take the row header 3 (because that is the element we have chosen), and follow the row right until we reach 3. From there, we follow the column up to the number in bold. That number is 1. So 1 is the identity for *,(mod 5), and as a matter of fact, 1 is ALWAYS the identity element for traditional modular multiplication, just as 0 is always the identity element for traditional modular addition and subtraction.

Now for the inverses. Now be careful that you don't confuse inverses for multiplication of the reals with inverses for multiplication under a modulus. Although both sets share an identity element of 1, the inverse elements for identical numbers are different. For example, in $\mathbb{R}, 3^{-1} = \frac{1}{3}$. However, the number $\frac{1}{3}$ does not exist in the world of (mod 5). The only numbers that do exist are 0,1,2,3,4. So, if an element has an inverse, it must be one of those numbers.

Now, the definition states that the inverse of k, denoted k^{-1}, is an element such that $k * k^{-1} = e$. We also know that the inverse of a set is not unique- each element has its own inverse that is not shared by any other element. Let's look at the inverses for multiplication (mod 5), remembering that in this case $e = 1$:
$1 \implies 1*1^{-1} = 1$ To find this, we follow the bold number 1 to the right until we reach

the number 1. Then we follow the table up until we reach the bold row header. It turns out that under multiplication (mod 5), $1^{-1} = 1$.
$2 \Longrightarrow 2 * 2^{-1} = 1$ Again, follow the bold 2 to the right until you reach the number 1. Following the table up to the top, we see that $2^{-1} = 3$.
$3 \Longrightarrow 3 * 3^{-1} = 1 \rightarrow 3^{-1} = 2$
$4 \Longrightarrow 4 * 4^{-1} = 1 \rightarrow 4^{-1} = 4$

A quick note- if a is the inverse of b, then b is the inverse of a. Finally, you probably notice that we left one element out. There is no element that when multiplied by 0, gets you back to 1. This tells us that 0 has no inverse under modular multiplication. So, you can see that certain elements have no inverse. While this has algebraic significance, we will not explore this concept until the final chapter of the notes. Now, one more table:

$*$, (mod6)	**0**	**1**	**2**	**3**	**4**	**5**
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	2	4
5	0	5	4	3	2	1

Do you see how this one differs from the example for (mod 5)? If you look at the elements 2,3 and 4, you'll see that the number 1 does not appear in any of those rows. This tells us that those elements do not have an inverse (mod 6). Is there a way to determine whether or not an element has an inverse (mod m) without constructing a table? Of course there is!

THEOREM (4.5.4)- Given an element k(mod m) with the operation multiplication. If $(k, m) = 1 \rightarrow \exists k^{-1}$(mod m). If $(k, m) \neq 1$, then no inverse exists.
Proof- If $(k, m) = 1$, then we can find a, b s.t. $ka + mb = 1$. Now, we want to prove that there exists a k^{-1} s.t. $k * k^{-1} = 1$(mod m). Let's apply (mod m) to the equation $ka + mb = 1$ and reduce. This gives us the equivalence $ka + 0 = 1$ because m multiplies by any number is equal to 0(mod m). So we end up with $ka = 1$(mod m), which tells us that $k^{-1} = a$. Now, if $(k, m) \neq 1$, we can say $(k, m) > 1 = d \neq 1$. Thus $d|k$ and $d|m$. Now look at $k * k^{-1} = 1$(mod m). By our definition of congruence, that gives us $m|(k * k^{-1} - 1)$ or $ml - k * k^{-1} = 1$. But this is not possible. Since d divides both terms on the left side, it must divide 1, but we have already stated that $d > 1$, which is a contradiction. So if $(k, m) > 1 = d \rightarrow$ no k^{-1} exists.

■

What can we do with all of this? We can now determine whether or not a linear (no squares or cubes or higher exponents) congruence has a solution (mod m). Essentially.....

<u>**THEOREM (4.5.5)**</u>- Let $a, b \in \mathbb{Z}, m \in \mathbb{Z}^+$, and $(a, m) = d$. If $d \nmid b$, then $ax \equiv b(\text{mod } m)$ has no solutions. If $d|b \longrightarrow ax \equiv b(\text{mod } m)$ has exactly d incongruent solutions (mod m).

We have basically proven the first part of this theorem in (4.5.4), but the second part is new. Don't be sad, but we won't be proving this.

<u>ex</u>: Solve for $x : 4x \equiv 3(\text{mod } 5)$
Before we solve this equivalence, let's look at what we would do if the (mod 5) wasn't there. We'd simply have $4x = 3 \rightarrow x = \frac{3}{4}$. But how would we get there? We would take the inverse of 4, which is $\frac{1}{4}$, and multiply on both sides. Another way of looking at it is saying $4^{-1} * 4x = 4^{-1} * 3$. This is precisely what we will do in the equivalence, only this time $4^{-1} = 4(\text{mod } 5)$. So we have this: $4x \equiv 3(\text{mod } 5)$ $\rightarrow 4^{-1} * 4x \equiv 4^{-1} * 3 \rightarrow x \equiv 4 * 3 \rightarrow x \equiv 12 \equiv 2(\text{mod } 5)$. So that's our answer, and plugging back into the original equivalence will show that it works.

Now, the question might arise as to whether or not 2 is the only answer. And that depends on how you look at the question- while it is true that 7 and 12 and 17, etc. will all prove the equivalence true, there is only one correct answer in the world of (mod 5). Of course that answer is the least non-negative residue of all those solutions, which is 2.

<u>ex</u>: Solve for $x : 9x \equiv 12(\text{mod } 15)$
The first thing we want to do is check if there are any solutions, and if so, how many there will be. So we go back to theorem (4.5.5) to check $(9, 15) = 3$. Since $3|12$, there are exactly three solutions to this linear equivalence. The next thing we will do is divide 3 from both sides to get $3x \equiv 4(\text{mod } 5)$. We want to find $3^{-1}(\text{mod } 5)$. By checking our table, we can see that $2 = 3^{-1}(\text{mod } 5)$. Multiplying both sides by 2 gives us $x \equiv 4 * 2 = 8 \equiv 3(\text{mod } 5)$. Plugging this back in should convince you of the solution's validity. However, theorem (4.5.5) tells us that there are 3 solutions, and we've only found one. The other two solutions come from adding $\frac{m}{d}$ to our initial answer, and then adding it again. So the three solutions to this linear equivalence are 3,8, and 13. Plug them in if you don't believe me.

One last thing before we end the section- it is silly to think that we will always have a Cayley table close at hand to look up inverses. In cases where the numbers are sufficiently large and there is no table handy, we have to come up with a new way

to find inverses. Here is quick outline of what to do if you are looking for the inverse of some element k:
(1) Write out multiples of the modulus
(2) Add one to each of the multiples from (1)
(3) Find the smallest number from (2) that is divisible by k
(4) Divide the number found in (3) by k. That is your inverse!

ex: Find the inverse of 13(mod 18)
We take multiples of 18 and add 1 to each until we find a number divisible by 13: 19, 37, 55, 73, 91. Since $\frac{91}{13} = 7$, 7 is the inverse of 13(mod 18)

Exercises

1. Show that if $p \geq 3$ is prime, then $18|(p^6 - 1)$.
2. Prove that if an integer is a perfect square, then it is congruent to 0 or 1 (mod 4)
3. Is the number 333333333333333333333333334 a perfect square?
4. Using any technique you are comfortable with, solve for x in each of the following: ((d) is the important one, though)
   (a) $4! \equiv x(\text{mod } 5)$
   (b) $6! \equiv x(\text{mod } 7)$
   (c) $10! \equiv x(\text{mod } 11)$
   (d) $100! \equiv x(\text{mod } 101)$
5. Come up with a rule that generalizes the process used in question 1.
6. Prove divisibility by 3 using mods.
7. Attempt to come up with a rule for divisibility by 11 using the same technique as the one used in Theorem (4.5.2).
8. Solve for x as an LNR:
   (a) $3^{1000} \equiv x(\text{mod } 80)$
   (b) $5^{81} \equiv x(\text{mod } 60)$
   (c) $4^{667} \equiv x(\text{mod } 13)$
   (d) $7^{50} \cdot 4^{102} \equiv x(\text{mod } 110)$

9. What is the last digit of the number $9^{11111111111111}$?

10. What are the last three digits of the number $7^{500} * 11^{501} * 13^{502}$

11. What are the inverses for each element in the table (+,(mod 4))?

12. Write out addition tables for (mod 6) and (mod 9)

13. Write out multiplication tables for (mod 8), (mod 9) and (mod 12)

14. Find the inverses elements for each of the tables in the previous question.

15. For which integers $n : 0 \leq n \leq 40$ does the congruence $12x \equiv n \pmod{30}$ have solutions?

16. What is the inverse under multiplication (mod 9) of the numbers 5,6,7, and 8?

17. Solve the following linear congruences:

    (a) $3x \equiv 2 \pmod{7}$

    (b) $7x \equiv 4 \pmod{12}$

    (c) $8x + 4 \equiv 11 \pmod{15}$

    (d) $9x \equiv 5 \pmod{25}$

18. Think about the connection between linear congruences and linear diophantine equations. How are the two concepts related. Can you find a way to translate one into the other?

19. Which integers yield a remainder of 1 when divided by 2 or 3?

20. Find three integers that satisfy the following congruences:
    $x \equiv 2 \pmod{3}$
    $x \equiv 2 \pmod{5}$
    .....and $4|x$

Now we completely switch gears to a topic that has absolutely nothing to do with anything we have covered up to this point. Whereas many previous sections had you performing somewhat complex calculations, this chapter will rely more on your ability to interpret questions and think your way to a solution. That is not to say that there are no formulas or theorems, but here they will take on a slightly different form.

This chapter deals with the myriad ways you can count objects. Counting in math is precisely what it sounds like- the process by which we figure out the number of objects in a set. You have probably encountered some of these counting topics at an early point in your math life- you've no doubt calculated combinations and permutations and fretted over when order "matters" or doesn't. We will attempt to count some pretty complex arrangements, and then translate those counting arguments into an entirely new type of proof- the combinatorial proof. But first, as always, we establish these new concepts with some definitions and theorems.

(5.1) – Counting

Definition- The process of **ENUMERATION** is the counting technique whereby every element in a set is listed.

This is the most basic counting technique. Listing all numbers or combinations or orderings is both tedious and impractical. Still, it is a valid technique if at all feasible.

ex: Enumerating all positive odd numbers less than 10 is the list 1,3,5,7,9.

THEOREM (5.1.1)- Suppose a procedure can be broken down into a sequence of k tasks. If there are n_1 ways to complete the first task, n_2 ways to complete the second task..... then there are $n_1 n_2 .....n_k$ ways to complete the procedure. We call this process the *Product Rule.*

Proof- As with many counting procedures, we will not prove this explicitly. The reason for this is simple- theorems such as this are better explained with tree diagrams that will be shown in class.

ex: A student owns three shirts, two pairs of pants, and five hats. If the students must wear one of each to school, from how many different outfits can the student choose?
This one is an easy one- it's simply 3*2*5=30 possible outfits.

ex: How many different four-digit numeric passwords can be constructed from the numbers 0-7 if repetition is allowed?
We have 8 choices for the each of the four characters, so the answer is $8*8*8*8 = 8^4$ possible passwords.

ex: What if, in the previous example, repetition is not allowed?
This is a bit more difficult, but not by much. We would have 8 possible choices for the first number, and then because we cannot repeat a number, 7 possible choices for the second, 6 for the third, and 5 for the fourth. That gives us 8*7*6*5 possible passwords.

Note that in counting questions, we don't always care about a numeric answer; the process is much more important than doing tedious calculations. If we used calculators in this course, this would be the time to bust them out..... but of course we don't use calculators in this course.

THEOREM (5.1.2)- Suppose a task can be done in either $n_1, n_2.....n_k$ number of ways, where $\cap_{i=1}^{k} n_i = \emptyset$. Then there are $\sum_{i=1}^{k} n_i$ ways to complete this task. We call this procedure the *Sum Rule.*
Proof- Again, this one is better proven with a simple tree diagram that will be made clear in class.

Now, this one is a little tougher to grasp than the Product Rule. The first point of confusion may be the *cap*, but all that is saying is that none of the tasks can overlap, or that their intersection is empty. The second point of confusion may be what the heck the theorem is actually saying. Basically, if there are a bunch of items that you must choose between, and none of those items fall into more than one category, then simply add the number of objects in each category. An example or two will make this very clear.

ex: Say you are planning a trip from New York to Los Angeles. Looking at your travel options, you see that there are five different flights and three different train lines that will take you to your destination. How many different ways are there for you to get from NY to LA?
Easy. You can't choose more than one plane or train. You can only take one. So you have 5+3=8 options.

ex: Look at our previous example where you want to travel from NY to LA. Now let's assume that you have to make a stop-off in Chicago. These are the travel options: From NY to Chicago, there are four flights, two trains and eight buses. From Chicago to LA, there are two flights or five trains. How many total travel options are there? Now that we have a feel for the product and sum rules, we can try examples that combine the two.

This is a case where we have to go from NY to Chicago AND from Chicago to LA. For each of those two trips, there are separate options. There are 4+2+8=14 ways to get from New York to Chicago and 2+5=7 ways to get from Chicago to Los Angeles. For each of the 14 trips to Chicago, we can then choose one of the 7 ways to get to LA. This means that there are 14*7=98 different travel options.

ex: A password can be between 6 and 8 characters long, where the last character is a number, but everything before is a letter. How many different passwords are possible under these rules?
This one is much more difficult. We can create separate cases for the number of characters in the password and then add the results. If the password is six characters, there are 10*26^5 possibilities. If the password is seven characters, there are 10*26^6 possibilities, and if it is eight characters, we have 10*26^7 possibilities. Since each one of these cases is independent of each other, we can add the results to get $10(26^6 + 26^7 + 26^8)$ total possibilities.

As you can see, most of the difficulty in using these theorems is determining *which one* to use. Here is a good rule of thumb: If you see the word "AND" in the question, use the product rule, and if you see the word "OR", use the sum rule. But be careful that there is no overlap between the various sets or tasks in the question. Look at the following example that illustrates this point:

ex: You enter a dealership looking for a vehicle to lease. There are 20 cars in the dealership, and 15 red vehicles. How many different vehicles are there for you to purchase?
The ambiguous wording of the question might make it obvious that the answer isn't simply 35. This is, of course, because there is the possibility that some of those red vehicles are cars. All that we know for sure is that the dealership contains between 20 (if all the cars are red) and 35 (if none of the cars are red) vehicles.

The problem with counting in the previous example is that there is the possibility of overlap. In the case of overlap, we end up counting the same thing twice. So it would seem logical that we can deal with this overlap by simply subtracting the objects that appear more than once. Is it that simple, however? In math, it's never that simple. We can create complicated examples that require a greater deal of sophistication, but there are times when a bit of analysis and a little subtraction will tackle the problem.

ex: You have a choice between picking an even number less than 20 or a number between 0 and 10, inclusive. How many numbers are there for you to choose?
Obviously there are 15 numbers- 0 to 10, 12,14,16,18. But if we want to apply our new "subtraction principle", we would add 10 and 11 to get 21 total numbers, and then subtract the overlap, which is the six even numbers frmo 0 to 10. So the solution, as we knew it would be, is $10 + 11 - 6 = 15$.

ex: How many positive integers between 1 and 100 are:

1. Divisible by 6?
2. Divisible by 8?
3. Divisible by 6 and 8?
4. Divisible by 6 or 8?
5. Divisible by 6 or 8 but not both?

In attempting questions such as these, it is often helpful to construct a Venn Diagram. In this case, a Venn Diagram would be two overlapping circles. It is a useful exercise to try and determine what each section of the Venn Diagram represents.

Before answering these questions, we will introduce a formula that makes things much easier.

$\star$ If a and b are both divisible by d, then there are $\frac{b-a}{d} + 1$ numbers in the interval (a, b) that are divisible by d.

1. Of course you could simply enumerate each of the numbers divisible by 6. Those numbers are 6,12,18,24..... We want to find a better way, however. The best way to handle this is to "shrink the interval" so that it goes from the smallest number divisible by 6 to the largest number divisible by 6, and use the process from above. Since we are examining the numbers between 1 and 100, we will shrink the interval to the numbers 6 through 96. Thus $a = 6, b = 96$, and d, of course, is 6. Apply the formula to get $\frac{96-6}{6} + 1 = 15 + 1 = 16$ numbers between 1 and 100 divisible by 6.

2. Shrink the interval to 8 through 96, and apply the formula to get 12 numbers divisible by 8.

3. Numbers that are divisible by both 6 and 8 are also divisible by the LCM of the two numbers, which is 24. Applying the formula gives us 4 numbers.

4. This is the question where we end up applying the subtraction principle. To find all numbers divisible by either 8 or 6, we first find all numbers divisible by 8, then all numbers divisible by 6 and add them together. But we have overlap in that sum, because we have counted numbers divisible by 24 twice. (Why?) So we simply subtract the numbers divisible by 24. Of course, we have already solved for all of these values in parts (1), (2), and (3). Our solution is 16+12-4=24.

5. We now want either 6 or 8 but not both. This means that we want no numbers that are divisible by 24. So we can start by adding our solutions for (1) and (2), but we have overcounted by adding the numbers divisible by 24 two times each. So we subtract the numbers divisible by 24 twice. This gives us 16+12-2(4)=20.

We will end the section with one more question. The difficulty will be in trying to figure out which technique to use.

ex: A family consists of five boys and five girls. How many ways are there to arrange them for a photo if:

1. We alternate boys and girls in the photo?

2. A boy must be on both ends?

3. No two boys can be adjacent?

These are exercises you should attempt on your own before peeking at the answer. Remember that it is often useful to just apply common sense- think of how you would literally count out the possibilities for the various scenarios.

1. There are 10 possible family members who can occupy the first position, girl or boy. But once you have chosen who is first, the opposite sex must come next, leaving us with 5 possibilities for the second positiion. From then on, we are simply alternating family members of the opposite sex, and our answer is $10 * 5 * (4!)^2$.

2. We have five choices for the first position, and then once a boy has been placed, we have four choices for the final position. In between there are no restrictions, meaning that there are 8 possibilities for the second position, 7 for the third, 6 for the fourth, etc. Our solution is $5 * 4 * 8!$.

3. This question might seem easy, but it actually requires a pretty complex series of steps, using techniques that you haven't been taught yet. Your goal at this point should be to attempt to figure out why that is, or why it isn't as easy as the other two.

ex: Using letters a through d inclusive and the numbers from 0 to 5 inclusive, how many different six character passwords can you form if a password must contain at least one number?
I don't know that intuition gives a clear picture of which technique should be used in this problem. Can you do this by cases depending on how many numbers are in the password? Well, yes you can, but then you would have to figure out where the numbers fell in the password, and that requires a technique that will be taught in the next section. Instead, we will tackle this problem a little differently. Think of it this way: There are two possibilities when it comes to listing all possible passwords. A password can contain at least one number or it can contain no numbers. A password that contains no numbers contains only letters. So a password can contain at least one number or it can contain only letters. If we subtract the case where there are only letters, we get the statement "The number of total passwords minus the number of passwords containing only letters equals the number of passwords in which at least one number is present". A quick calculation tells us that there are 10^6 total passwords if anything goes. If we eliminated numbers, there are 4^6 passwords. So the number of passwords containing at least one number is $10^6 - 4^6$.

Unsurprisingly, we call this process *subtracting the complement.* Sometimes instead of counting the thing we want, it is much easier to count the thing that we don't want. You should think about subtracting the complement when the enumeration you desire consists of multiple, difficult to compute cases.

Exercises

1. There are 18 mathematics majors and 325 computer science majors at a college.
   (a) In how many ways can two representatives be picked so that one is a mathematics major and the other is a computer science major?
   (b) In how many ways can one representative be picked who is either a mathematics major or a computer science major?
2. An office building contains 27 floors and has 37 offices on each floor. How many offices are in the building?
3. A multiple-choice test contains 10 questions. There are four possible answers for each question.

   (a) In how many ways can a student answer the questions on the test if the student answers every question?

   (b) In how many ways can a student answer the questions on the test if the student can leave answers blank?

4. A particular brand of shirt comes in 12 colors, has a male version and a female version, and comes in three sizes for each sex. How many different types of this shirt are made?

5. Six different airlines fly from New York to Denver and seven fly from Denver to San Francisco. How many different pairs of airlines can you choose on which to book a trip from New York to San Francisco via Denver, when you pick an airline for the flight to Denver and an airline for the continuation flight to San Francisco?

6. There are four major auto routes from Boston to Detroit and six from Detroit to Los Angeles. How many major auto routes are there from Boston to Los Angeles via Detroit?

7. How many different three-letter initials can people have?

8. How many different three-letter initials with none of the letters repeated can people have?

9. How many different three-letter initials are there that begin with an A?

10. How many bit strings are there of length eight?

11. How many bit strings of length ten both begin and end with a 1?

12. How many bit strings are there of length six or less, not counting the empty string?

13. How many bit strings of length n, where n is a positive integer, start and end with 1s?

14. How many 5-letter sequences

    (a) end with A?

    (b) start with T and end with G?

    (c) contain only A and T?

    (d) do not contain C?

So we've introduced some basic counting principles that can tackle a rather narrow array of counting questions. Now it's time to get more serious, and actually come up with some formulas that will help us with slightly more complex problems. We will not necessarily derive these formulas until a later section, so try not to be too disappointed.

(5.2) – Permutations and Combinations

Up to this point, we have asked questions like "How many ways can we.....?" or "How many ways can we do this if we must choose ONE OF EACH?" Of course the way the problems are stated are a bit more subtle, but it has always come down to picking objects individually. For example, when counting passwords, we looked at each character individually and then multiplied the results. This is all well and good, but what if we want to count groups of objects? Then things aren't so easy. Look at the following question:

Q: How many different ways are there to order the set of numbers $\{1, 2, 3\}$?
A: Let's enumerate the possibilities- $\{1, 2, 3\}, \{1, 3, 2\}, \{2, 1, 3\}, \{2, 3, 1\}, \{3, 1, 2\}, \{3, 2, 1\}$. That's all of them and so there are six possibilities.

Like we said in the previous chapter- enumeration will always get you a solution, but it is rarely the most elegant way to do so. So think of it this way:

THEOREM (5.2.1)- The number of ways to order n objects is $n!$
Proof- Think of the n positions of the n objects. There are n possible objects that can be placed in the first position. Since we are ordering n objects, repetition is not allowed, and so there are $n - 1$ objects that can be placed in the second position. We continue in this way until there is only one position and one object left. Since we are placing each object individually, the product rule yields the equation $(n)(n - 1)(n - 2).....(2)(1) = n!$

■

ex: How many ways are there for five friends to stand in a line?

Easy- 5!

So that's how you would order every object in a set. For convenience in the future, we will use the notation $[n]$, to denote the set of all integers from 1 to n, or $\{1, 2, 3, 4.....n-1, n\}$. Now, what if you only wanted to take a finite number of elements in $[n]$, and then order them? The question becomes more difficult.

ex: How many ways are there to order two elements from [3]?
We can just enumerate the sets- $\{1, 2\}, \{1, 3\}, \{2, 1\}, \{2, 3\}, \{3, 1\}, \{3, 2\}$. So there are still 6 ways to order two elements from a three element set.

Now we would like to come up with an general way to calculate how to order k elements of an n element set. The following may have been given to you as a definition or a formula in high school, but here we will prove it as a theorem.

Definition- A **PERMUTATION** is the an ordering of elements in a set.

THEOREM (5.2.2)- There are ${}_nP_k$, or $(n)_k = \frac{n!}{(n-k)!}$ ways to order k elements in an n element set.
Proof- We start with a set containing n elements. If we again think of our orderings as a set of individual positionings, there are are n objects we can place in the first spot, and $n-1$ objects we can place in the second spot. This goes on until all k objects are placed. Using the product rule, we can write this as $(n)(n-1).....(n-k+1)$. But this quantity is exactly $\frac{n!}{(n-k)!}$

Q.E.D.

As you can see from the previous example, $(3)_2 = \frac{3!}{1!} = 6$.

ex: How many ten letter "words" are possible if you can't repeat letters?
sl'n: $(26)_{10}$

ex: Eight students are trying out for four different parts in a play. How many ways can these students be given parts?
sl'n: ${}_8P_4$

Of course, you can't tackle permutations without talking about combinations. And, as you no doubt remember from high school, while permutations are a way of counting where "order matters", a combination is a way to count where "order doesn't matter". So here goes:

Definition-A **COMBINATION** is a list of objects in a set.

THEOREM (5.2.3)- There are ${}_nC_k$, or $\binom{n}{k} = \frac{n!}{(k!)(n-k)!}$ ways to list k objects from an n element set.

Proof- This is trickier than the permutation proof, because it uses the previous proof and expands upon it. We may get a better understanding of how to prove this by looking at [3] and trying to create lists of 2. Here are the two-lists of $[3] - \{1,2\}, \{1,3\}, \{2,3\}$. Of course order doesn't matter in this case, so $\{1,3\} = \{3,1\}$. And that's the heart of the proof- a combination is simply a permutation where we divide out the number of orderings of each list. In this case, there are 2 orderings per list, so $\binom{3}{2} = \frac{(3)_2}{2!}$. In general, there are $k!$ ways to order k objects, so we get $\binom{n}{k} = \frac{(n)_k}{k!} = \frac{n!}{(k!)(n-k)!}$.

Q.E.D.

A VERY important thing to note about the previous proof is that we can only divide out the number of orderings because each list has the SAME number of orderings. For example, every single 3-set of [4] can be ordered in 3! different ways. If this were not the case, then we could not divide out 3!.

ex: Eight students are trying out for the part of four lamp posts in the school play. How many ways can those parts be assigned?
Ans: $\binom{8}{4}$, because one lamp post is the same as any other.

ex: You have ten school friends and eight camp friends. If you can bring three school friends and two camp friends on a trip, how many ways can you choose your friends for the trip?
Ans: We want two camp friends AND three school friends, so we will need to use the product rule. In each case, we don't care about the order in which the friends are chosen, so the solution is $\binom{10}{3}\binom{8}{2}$.

ex: A board has three positions for men. The board also wishes to hire a female president and treasurer. If there are ten men and six women applying for these positions, how many ways can they be filled?
Ans: We want two women where order matters AND three men where order doesn't matter. So we will multiply a permutation by a combination. The solution is $\binom{10}{3}(6)_2$.

Here is a question that will truly test your understanding up to this point:
Q: Given a standard deck of 52 cards with 13 types and 4 suits, in a five card draw, how many ways can you get:

1. 4 of a kind?

2. a flush?

3. a full house?

4. two pairs?

5. 3 of a kind?

These questions involve mostly every single technique you have learned in the past two sections. Part of the challenge, of course, is knowing when and where to use each technique.

1. There are 13 possibilities for the card that will appear four times, and only 1 way to draw all four of them. For the final card, there are 48 possibilities. So there are 13*48 ways to draw four of a kind.

2. A flush consists of five cards from the same suit. There are 13 cards in each suit and 4 suits, so there are $4\binom{13}{5}$ ways to get a flush.

3. A full house consists of three cards of one type and two of another. So, there are 13 choices for the first type, and $\binom{4}{3}$ ways to draw those cards. For the second type of cards, there are 12 choices for the type and $\binom{4}{2}$ ways to choose from that type. So, there are $13\binom{4}{3} * 12\binom{4}{2}$ possible full houses that can be dealt.

4. The problem with two pairs is that the fifth card dealt cannot be the same type as one of the original four, or else we have a full house. So, we are looking at $13\binom{4}{2} * 12\binom{4}{2} * 44$ ways to get two pairs.

5. The same issue applies here.....once we have chosen which type appears three times, we have to be careful that the remaining two cards are of completely different types. We don't want to accidentally draw three of a kind, four of a kind, or a full house. There are $13\binom{4}{3} * 48 * 44$ ways to get three of a kind.

As you can see, some of these counting problems can get very complicated. You have to be very careful that you don't *overcount*, or list a possibility more than once, when attempting to come up with an answer. As you grow in proficiency, this will occur less and less frequently, and you will begin to see the logic in why we use the methods we do. Half of the fun is trying to figure out easy ways to count something that seems difficult. A few further theorems will help with that.

THEOREM (5.2.4)- $\binom{n}{k} = \binom{n}{n-k}$
Proof- To convince yourself that this is true, simply try it with numbers like $\binom{5}{2} = \binom{5}{3} = 10$. Now, there are a few different ways we can prove this. We will use something called a combinatorial proof in a later section, but for now will we try it two diffferent ways: Algebraically and through a bijection.

1. Completing an algebraic proof is as simple as equating both sides after using our formula for ${}_nC_k$.
$\binom{n}{n-k} = \frac{n!}{(n-k)![n-(n-k)]!} = \frac{n!}{(n-k)!(k!)} = \binom{n}{k}$ Done.

2. Now to prove it via bijection: We need to find a function that is both one-to-one and onto that maps the elements in $\binom{n}{k}$ to the elements in $\binom{n}{n-k}$. Before proceeding, we should look at an example with small numbers, like $\binom{5}{2}$ and $\binom{5}{3}$ taken from [5] to see if we can find a function that maps the elements from one to the elements from the other.

3-sets of [5]	2-sets of [5]
$\{1,2,3\}$	$\{1,2\}$
$\{1,2,4\}$	$\{1,3\}$
$\{1,2,5\}$	$\{1,4\}$
$\{1,3,4\}$	$\{1,5\}$
$\{1,3,5\}$	$\{2,3\}$
$\{1,4,5\}$	$\{2,4\}$
$\{2,3,4\}$	$\{2,5\}$
$\{2,3,5\}$	$\{3,4\}$
$\{2,4,5\}$	$\{3,5\}$
$\{3,4,5\}$	$\{4,5\}$

Well, there are ten of each, but we knew there would be. The goal is to find a bijection that maps the sets in the left column to those in the right column. Do you see it? If not, it may be easier to see when written this way:

3-sets of [5]	2-sets of [5]
$\{1,2,3\}$	$\{4,5\}$
$\{1,2,4\}$	$\{3,5\}$
$\{1,2,5\}$	$\{3,4\}$
$\{1,3,4\}$	$\{2,5\}$
$\{1,3,5\}$	$\{2,4\}$
$\{1,4,5\}$	$\{2,3\}$
$\{2,3,4\}$	$\{1,5\}$
$\{2,3,5\}$	$\{1,4\}$
$\{2,4,5\}$	$\{1,3\}$
$\{3,4,5\}$	$\{1,2\}$

Now it becomes much clearer: The bijection we are looking for is simply mapping a 3-set to its complement! Now that we have given the function, we leave the proof of bijection as an exercise at the end of the chapter.

■

Now let's return to the formula for a combination, which involves dividing out the orderings of a list so we are just left with the actual elements. We stated that you can only divide out the arrangements if every single list has the same number of arrangements. Look at the following question:

Q: How many ways can the word DADDY be permuted?
A: Any ideas? We might want to say 5! because there are 5 elements, but this won't work because the multiple Ds will cause an overcount. Let's start by enumerating the possibilities: DADDY, DDDAY, DDDYA, ADDDY, YDDDA , AYDDD, YADDD, DDADY, DDYDA, DDAYD, DDYAD, ADDYD, YDDAD, DYDDA, DAYDD, DYADD, ADYDD, YDADD, DADAY, DYDAD. So there are 20 possible permutations. But is there any way to get that with a formula?

We know interchanging the Ds does not change our permutation, so let's keep track of the Ds and see how many permutations end up being the same: $D_1AD_2D_3Y = D_1AD_3D_2Y = D_2AD_1D_3Y = D_2AD_3D_1Y = D_3AD_1D_2Y = D_3AD_2D_1Y$ So it looks like if we choose the position of the Ds (in this case, position 1,3, and 4) then the number of orderings remains constant. Namely, there are always 6=3! orderings. So while there would normally be 5! ways to order these letters, because of the three interchangable objects, there are actually $\frac{5!}{3!} = 20$ permutations possible.

THEOREM (5.2.5)- If a procedure can be carried out in n ways, and for every way w, exactly d of the n ways correspond to the way w, then there are $\frac{n}{d}$ unique ways to complete the task. We call this process the *Division Rule.*
Proof- We showed how this works in the previous example, so we will forgo a bijective proof in this space. However, for the sake of understanding what is a pretty confusing theorem, we will explain what each letter represents in terms of the above example. n is equal to the number of permutations we would have if there were no interchangable item which in this case is 120. w is equal to a particular arrangement of letters; for example, an arrangement where D occupies the 1st, 3rd and 4th positions in the word. Finally, the d is the number of orderings of the interchangable letters, which here would be 3!=6.

ex: How many ways can the word MISSISSIPPI be permuted?
We have more than one interchangable letter, but this will not affect our answer. We treat each of them separately and apply the product rule in the denominator. Our solution is $\frac{11!}{4!4!2!}$.

ex: How many different ways are there to seat four people around a circular table, where two seatings are considered the same when each person has the same right and left neighbor?

This one can seem nasty at first, but is actually not so terrible if you see the trick. We know that if there weren't interchangable seatings, then there would be 4! ways to seat 4 people. But we DO have interchangable seatings, and we need to divide them out. How many interchangable seatings? There are 4, one for each rotation around the table. So that leaves us with $\frac{4!}{4}$ different seatings.

Up to this point, we have only been dealing with counting in which there is no repetition. That's a bit of a lie, as in the previous section, I slipped a few in there because I knew you were ready for it. Yes, you. Now we are all ready to expand our counting techniques by formalizing what we do when repetition IS allowed.

THEOREM (5.2.6)- If there are n objects to choose from, and we wish to make a list of k items, there are n^k such lists.
Proof- Not much to say here. We treat each item on the list separately, and use the product rule. There are n choices for each item, and we want k of them, so we get $n * n * n * ..... * n, k$ times. Or n^k.

There isn't much that needs to be said about this, as we've already done examples. Let's complicate things.

Q: How many ways are there to pick 4 pieces of fruit from a bowl with an infinite number of apples, oranges and pears?
Ans: Right now we have no idea how to tackle this kind of question. It isn't a simple permutation because nothing about order is mentioned in the question. And it's not a simple combination because of the repetition qualifier. So as always, we will enumerate the answer, and see if that helps. (In this case, it probably won't) We will call apples A, oranges O, and pears Q. Just kidding; we will call them P.

AAAA, OOOO, PPPP, AAAO ,AAAP, OOOP, PPPA, PPPO, AAOO, AAPP, OOPP, AAOP, OOAP, PPAO. That's all of them. 15.

Like I said, this probably didn't help much. But look at what happens if we make "piles" of the fruit that we are choosing. We will separate each fruit (which we will denote by *) into its own pile, and separate each pile by a | symbol. The apples will be the first pile, the oranges the second pile, and the pears the third pile. Here are a few examples of what I mean:

4 Apples- $* * * * ||$
2 Apples, 2 Pears- $* * || * *$
1 Orange, 3 Pears- $| * | * **$
1 Apple, 2 Oranges, 1 Pear- $*| * *|*$

Note that in each example, we have four *s and two |s. That's a total of 6 objects altogether. And every time we move the |s around, it gives us a unique choice of fruit. As a matter of fact, if we translate our enumeration to the "stars and bars" as we did above, we will get every possible ordering of |s and *s. This means that we can find all lists with repetition by using this star and bar method. So, for four fruit and three varieties, there are $\frac{6!}{4!2!} = \binom{4+3-1}{4} = 15$ ways to choose.

THEOREM (5.2.7)- There are $\binom{n+r-1}{r}$ ways to count r elements from a set with n objects if repetition is allowed. We call these counting objects *multisets.*
Proof- We will again forgo the bijective relationship that proves the theorem.

The most important thing to remember for this one is that n is the number of varieties and r is the number of elements you are choosing. More practice!

ex: How many ways are there to select six coins from a box filled with pennies, nickels, dimes, quarters and half-dollars?
Just apply the formula: $\frac{10!}{5!5!}$

ex: How many solutions are there to the equation $x + y + z = 10, x, y, z \in \mathbb{Z}^+ + \{0\}$? This is well-hidden multiset question. Here, the categories are the three variables x, y, z, and we are looking for ten of them. So our solution is $\binom{3+10-1}{10} = \binom{12}{10}$.

Exercises

1. How many permutations of (a, b, c, d, e, f, g) end with a?
2. Let S=(1,2,3,4,5)
   (a) List all the 3-permutations of S.
   (b) List all the 3-combinations of S.
3. How many possibilities are there for the win, place and show (1st, 2nd, 3rd) positions in a horse race with 12 horses if all orders of finish are possible?
4. How many subsets with an odd number of elements does a set with ten elements have?
5. A coin is flipped eight times where each flip comes up either heads or tails. How many possible outcomes
   (a) are there in total?

(b) contain exactly three heads?

(c) contain at least three heads?

(d) contain the same number of heads and tails?

6. How many permutations of the letters $ABCDEFGH$ contain

   (a) the string ED?

   (b) the string CDE?

   (c) the strings BA and FGH?

   (d) the strings AB, DE, and GH?

   (e) the strings CAB and BED?

   (f) the strings BCA and ABF?

7. Thirteen people on a softball team show up for a game.

   (a) How many ways are there to choose 10 players to take the field?

   (b) How many ways are there to assign the 10 positions by selecting players from the 13 who show up?

   (c) Of the 13 people who show up, three are women. How many ways are there to choose 10 players to take the field if at least one of these playters must be a woman?

8. How many 4-permutations of the positive integers not exceeding 100 contain three consecutive integers $k, k+1, k+2$ in the correct order

   (a) where these consecutive integers can perhaps be separated by other integers in the permutation?

   (b) where they are in consecutive positions in the permutation?

9. Suppose that a department contains 10 men and 15 women. how many ways are there to form a commitee with six members if it must have more women than men?

10. Prove the bijection given in the second part of Theorem (5.2.4).

11. Find all values of x that satisfy $\binom{31}{9} = \binom{31}{x}$.

12. How many different functions can be mapped from:

    (a) A set with 5 elements to a set with 3 elements?

    (b) $f : [5] \to [3]$ that is one-to-one?

   (c) An onto function from [5] to [3]? (this one is very difficult! should be attempted just for ”fun”)

13. How many positive integers less than 1000

    (a) are divisible by 7?

    (b) are divisible by 7 but not by 11?

    (c) are divisible by both 7 and 11?

    (d) are divisible by either 7 or 11?

    (e) are divisible by exactly one of 7 or 11?

    (f) are divisible by neither 7 nor 11?

    (g) have distinct digits?

    (h) have distinct digits and are even?

14. Repeat the previous question a-f with the numbers 6 and 8.

15. How many license plates can be made using either three digits followed by three uppercase English letters or three uppercase English letters followed by three digits?

16. How many different functions are there from a set of 10 elements to sets with the following number of elements?

    (a) 2

    (b) 3

    (c) 4

    (d) $n : n \in \mathbb{Z}^+$

17. In how many different ways can five elements be selected in order from a set with five elements when repetition is allowed?

18. How many strings of six letters are there?

19. How many ways are there to select five unordered elements from a a set with three elements when repetition is allowed?

20. How many different ways are there to choose a dozen donuts from the 21 varieties at a donut shop?

21. A bagel shop has plain muffins, cherry muffins, chocolate muffins, almond muffins, apple muffins, and um...... broccoli muffins. How many ways are there to choose

(a) a dozen muffins?

(b) three dozen muffins?

(c) two dozen muffins with at least two of each kind?

(d) two dozen muffins with at least five chocolate muffins and at least three almond muffins?

(e) two dozen muffins with no more than two broccoli muffins?

(f) two dozen muffins with at least one plain muffin, at least two cherry muffins, at least three chocolate muffins, at least one almond muffin, at least two apple muffins and no more than three broccoli muffins?

22. How many solutions are there to the equation $x_1 + x_2 + x_3 + x_4 + x_5 = 2$, where $x_i, i = 1, 2, 3, 4, 5$ is a nonnegative integer such that

(a) $x_1 \geq 1$?

(b) $x_i \geq 2$ for $i = 1, 2, 3, 4, 5$?

(c) $0 \leq x_1 \leq 10$?

23. How many different strings can be made from the letters in AARDVARK, using all the letters, if all three As must be consecutive?

24. How many strings with five or more characters can be formed from the letters in SEERESS?

25. If $x, y, z \in \mathbb{Z}$, and $x \geq 1, y \geq 2, z \geq 3$, how many solutions are there to the equation $x + y + z = 12$?

(5.3) – Combinatorial Proofs

The title of this section is a bit misleading. We are going to be doing algebraic and combinatorial proofs. You might like the algebraic ones better, but that's only because you have been doing algebra your whole life. While algebraic proofs get the job done, there is nothing elegant about them. You simply follow steps and set both sides equal to each other. Combinatorial proofs, as you will see, involve arguments that seemingly come out of nowhere, and yet are so much simpler and cleverer than any algebra. They are a bit difficult to understand at first, but once the comprehensional hurdles are cleared, you will see them as the best way to handle a counting proof.

THEOREM (5.3.1)- $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$
Proof- We will start by doing this proof algebraically.
$\binom{n}{k-1} + \binom{n}{k} = \frac{n!}{(k-1)!(n-k+1)!} + \frac{n!}{k!(n-k)!} \rightarrow$
$\frac{k}{k}\frac{n!}{(k-1)!(n-k+1)!} + \frac{n-k+1}{n-k+1}\frac{n!}{k!(n-k)!} = \frac{kn!}{k!(n-k+1)!} + \frac{(n-k+1)n!}{k!(n-k+1)!} = \frac{kn!-kn!+(n+1)n!}{k!(n-k+1)!} =$
$\frac{(n+1)!}{(k!)(n+1-k)!} = \binom{n+1}{k}$

■

So, that was the algebraic way of proving it. Nothing special. But there is another way to prove it.....

Definition- A **COMBINATORIAL PROOF** is a way to prove two sets of objects are equal by counting them in two different ways.

Now, that might not mean very much to you until you hear how to put it into action. The form of a combinatorial proof is an unusual one. You start by asking a question that is specific to the proof. This is perhaps the most difficult part of the entire process, as you will see when we do examples. Once you have formulated a question, you must figure out a way to answer that question in two completely different ways. You will answer the question by using counting techniques that you have learned. Since you have answered the question twice using different counting methods, the two methods must actually be the same. Now we will reprove Theorem (5.3.1) combinatorially.

THEOREM (5.3.1 Again)- $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$

Question- How many ways can you choose k friends for a trip if you have $n+1$ friends?
Left Side- By defintion of a combination, you can do this $\binom{n+1}{k}$ ways.
Right Side- If Dave is one of your $n+1$ friends, you can either choose to bring him or choose not to bring him. If you DO choose to bring him, then you still have to choose $k-1$ other friends from the remaining n friends. You can do this in $\binom{n}{k-1}$ ways. If you choose NOT to bring him, then you must choose k friends from the remaining n friends, which you can do in $\binom{n}{k}$ ways. Since those possibilities encompass EVERY single way you can choose your friends, there are $\binom{n}{k-1} + \binom{n}{k}$ ways to choose your friends.

Since we have counted the same quantity in two different ways, we know those two quantities must be equal.

■

Do you see the utility of employing this method? We didn't have to perform any tedious mathematical computations in order to finish the proof! It was a simple argument that was based on nothing other than a simple question about friends going on a trip together. It may not seem as though this is a valid construction, but it is just as valid as any other type of proof that we have attempted in this class. Now for more practice!

Oh yeah; about the theorem we just proved twice- it's actually called *Pascal's Theorem*, because it is the basis for Pascal's Triangle. If you remember from high school, Pascal's Triangle is the construction that allows us to pick the coefficients when we expand a binomial raised to a power.

THEOREM (5.3.2)- $\binom{n}{r} = \binom{n}{n-r}$
Proof- This time we will prove this combinatorially.
Question- How many ways can we choose k people for a job if there are n applicants?
Left Side- By definition, $\binom{n}{k}$.
Right Side- What if we were to choose the people NOT getting the job? We need to choose the $n-k$ people out of n, or $\binom{n}{n-k}$ people.

Q.E.D.

THEOREM (5.3.3)- $1 + (1)(1!) + (2)(2!) + (3)(3!) + ... + (n-1)((n-1)!) = n!$
Proof- This can be proven by induction, but.....
Question- How many different ways can we line up n friends in a row?
Right Side- $n!$ ways, by our definition in section 5.2.
Left Side- This one is a bit rough, so bear with it. Let's start by assuming that the friends are all different heights, and I wish to line them up from tallest to shortest. Of course, because I'm not so bright, there is a chance I'll get it all wrong. Here is

what might happen:
I might get it completely correct. There is only 1 way to line them up correctly....
OR
I might mess up the second to last guy. Well, that means I lined up the first $n-2$ correctly (there is only 1 way to do this), and then in the 2nd to last position, I placed the wrong guy. Because there are only two friends left at this point, there was only one incorrect choice for the 2nd to last position. So there are $(1)(1!)$ ways to mess it up this way.
OR
I might mess up the third to last guy. Then I lined up the first $n-3$ properly (1 way to do this), and messed up in the third to last position. Since there are three left and I've messed up, there are 2 possible wrong choices for who I placed in the third to last spot. Finally, there are 2! ways to order the last two friends, for a total of $(2)(2!)$ ways to mess it up this way.
OR
I could mess up the fourth to last friend. After getting the guys in the front correct, there are 3 incorrect choices for the fourth to last spot and 3! to place the final three. That makes a total of $(3)(3!)$ ways to count this scenario.
OR it goes on and on like this until...... I could mess up the 2nd guy, which means I placed the first correctly. There are$n-2$ wrong choices, and $(n-2)!$ ways to place the rest.
OR I could mess up the first guy. As you have figured out by now, there are $(n-1)(n-1)!$ ways to do this.

In total, there are $1+(1)(1!)+(2)(2!)+(3)(3!)+\ldots..+(n-1)((n-1)!)$ total ways to order your n friends.

■

THEOREM (5.3.4)- $\sum_{i=0}^{n}\binom{n}{i}=2^n$
Proof- We actually proved this in chapter 3, (when we learned about sets) but our process was a bit nebulous. We will now prove this combinatorially.
Question- If a set has n elements, how many subsets does it have?
Right Side- 2^n subsets, by a previous theorem.
Left Side- If a subset has 0 elements, there are $\binom{n}{0}$ subsets of that size. There are $\binom{n}{1}$ subsets of 1 element, etc. We simply sum the number of subsets over every possible number of elements.

Q.E.D.

BINOMIAL THEOREM (5.3.5)- $(x+y)^n=\sum_{j=0}^{n}\binom{n}{j}x^{n-j}y^j$
Proof- This is another one of those theorems you have used extensively in the past,

but I doubt you've ever known (or wondered) why it works. Well, combinatorics will take care of it rather quickly.
Question- How many n character passwords can you make if you are choosing from letters in english (which we call x), and letters in arabic (which we will call y)?
Left Side- By theorems and definitions in the previous section, $(x+y)^n$.
Right Side- Each password has a set number of english letter and a set number of arabic letters. Since the password must be n characters long, the sum of the number of english letters x and arabic letters y must be equal to n. Furthermore, if there are j arabic letters in the password, there must be $n-j$ english letters in the password. For example, if there is 1 arabic letter, then there are $n-1$ english letters, 2 arabic letters, $n-2$ english letters. So now we will sum through all the possible number of arabic letters that are in the password, from 0 to n. Each time we pick j arabic letters to be in the password, we must figure out where within the n character password to place them. That's where the $\binom{n}{j}$ comes in. We do not have to worry about where the english letters are placed, because once we haved chosen where to place the arabic letters, the english letters are fixed. So, in total, there are $\sum_{j=0}^{n}\binom{n}{j}x^{n-j}y^j$ passwords.

■

As always, playing around with numbers will make this much clearer. This time when you plug in, attempt to reconcile what you see with what is written in the theorem above. By now you can see how far-reaching combinatorial proofs actually are- they end up solving problems that you enver knew were problems in the first place. Now that we have proven the binomial theorem, there are a few other things we can learn directly from it:

THEOREM (5.3.6) Again Again- $\sum_{i=0}^{n}\binom{n}{i} = 2^n$
Proof- This time we will use the binomial theorem, with $x, y = 1$. $2^n = (1+1)^n = \sum_{i=0}^{n}\binom{n}{i}1^{n-i}1^i = \sum_{i=0}^{n}\binom{n}{i}$

Q.E.D.

THEOREM (5.3.7)- $\sum_{k=0}^{n}(-1)^k\binom{n}{k} = 0$
Proof- We are going to use the binomial theorem again, but this one may be more diffiicult to see. Just like in the previous theorem, we are going to start with the number on the right, 0. We ultimately want to get $(-1)^k$, so let's write 0 as $(1+(-1))$, so it fits the biniomial theorem. $0^n = (1+(-1))^n = \sum_{k=0}^{n}(1)^{n-k}(-1)^k\binom{n}{k} = \sum_{k=0}^{n}(-1)^k\binom{n}{k}$

Q.E.D.

Now that we've looked at a few different types of combinatorial proofs, it's time to look at one of my *favorite* types of combinatorial proofs. Namely, proofs involving the *tiling* of a 1xn checkerboard. In order to tackle these proofs, I suppose we need to informally define a few terms. When I say *checkerboard*, I am referring to a rectangle of alternating 1x1 white and black (or red and black, whatever you prefer) boxes. When I refer to a *domino*, I simply mean a 1x2 rectangle that can cover two boxes in a checkerboard, and when I mention a *square*, I am referring to a shape that covers a single 1x1 box on a checkerboard. Now that that is out of the way, let's get into it.....

<u>Definition:</u> The **TILING** of a checkerboard is the placing of various shapes on the board in such a way in such a way that every box is covered, no shapes overlap, and every shape is wholly contained within the confines of the baord.

Basically, a tiling is a way to cover a checkerboard in a natural way. For exampe, if you had an 8x8 (standard) checkerboard, you might tile it by placing 32 dominoes, four in each row. There are many ways to tile a standard checkerboard with squares and dominoes, but we will confine our examination to 1xn checkerbaords.

Our first goal will be to see if we can figure out how many different ways there are to tile a 1xn board. How might be go about trying to accomplish this goal? Remember, when attempting problems that have no obvious solution, plugging in numbers (in this case for n) might lead to some insight.

Case n=1: We are looking at a 1x1 checkerboard, and being asked to tile it with either squares or dominoes. Remember that a domino is a 2x1 rectangle, and a square is a 1x1 rectangle. Obviously there is only ONE possible tiling, and that is to place the square on the checkerboard.
Case n=2: We are now looking at a 2x1 checkerboard, which can be tiled either by placing two squares or a single domino. This leads to TWO tilings.
Case n=3: On a 3x1 checkerboard, we are still rather limited in our options. We can place three squares for our first tiling. Then we can place a single square and a single domino. As there are two ways to do this (domino on left, square on right or vice versa), we have THREE tilings overall.
Case n=4: Now things open up a bit, as we have a bunch of different ways for a tiling. Obviously we can place either two dominoes or four squares for the first two tilings. Or we can place a single domino and two squares on the checkerboard. There are three ways to do this, which you can see if you think about the position of the domino. It can be placed in boxes 1 and 2 or boxes 2 and 3 or boxes 3 and 4. This gives us a total of FIVE tilings.
Case n=5: This is the last case we will explain. Five squares yield the first tiling. We now have the option to place either one domino and three squares or two dominoes

and one square. There are four ways to place one domino and three squares, as seen by counting the possible positions of the domino. For the case of two dominoes and one square, it is easier to simply count the possible positions for the lone square. The square can either be in the first, last, or middle position. It cannot be placed in either the second or fourth box on the checkerboard. (Why?) So there are three tilings that have have two dominoes and one square. This gives us a total of 1+4+3=8 tilings.

It starts to get a bit out of hand from here, but that should come as no surprise- the longer your checkerboard, the larger the number of tilings. Now, perhaps you've noticed the pattern in the number of tilings as n increases. If you have not, I will explain one final case, that of a 0x1 checkerboard. Note that a 0x1 checkerboard isn't a board at all, but there is a way to tile it with squares and dominoes. Basically, the only tiling is that you can place zero dominoes and zero squares. This may seem silly, but it is a valid tiling, and thus when $n = 0$, there is ONE tiling of an 1x0 checkerboard.

Time to put it all together- here is a listing of n, and how many tilings we can make of a 1xn checkerboard:
$n = 0 \rightarrow 1$ tiling.
$n = 1 \rightarrow 1$ tiling.
$n = 2 \rightarrow 2$ tilings.
$n = 3 \rightarrow 3$ tilings.
$n = 4 \rightarrow 5$ tilings.
$n = 5 \rightarrow 8$ tilings.

When $n = 6$, there are 13 tiilngs, and you should be able to guess by now that when $n = 7$, there are 21 tilings. As amazing as it might seem, the number of tilings of an nx1 checkerboard is simply the n^{th} Fibonacci number! Oh, maybe I should define what that is exactly.....

Definition- The **FIBONACCI NUMBERS** are a sequence that is defined by setting $f_0 = 1, f_1 = 1$, and $f_n = f_{n-1} + f_{n-2}$

COMBINATORIAL BASE THEOREM- The number of tilings of an nx1 checkerboard is f_n.

We are going to use this fact as the LHS of many of our future combinatorial theorems.

THEOREM (5.3.8)- $f_n = f_{n-1} + f_{n-2}$
Though we just stated this as a definition, we can actually prove this is we use our Combinatorial Base Theorem along with a combinatorial proof.

Question- How many ways are there to tile an nx1 checkerboard?
Left Side- By our base theorem, there are f_n ways to tile the checkerboard.
Right Side- Let's ask the following question- was the last tile you placed a square or a domino? If you have an nx1 checkerboard, and the last tile you place is a square, it means that you have already tiled the other $(n-1)$x1 boxes in one of the f_{n-1} ways dictated by the base theorem. OR you could have placed a domino last, which means that you had already tiled the other $n-2$ squares in one of f_{n-2} ways. In total, there were $f_{n-1}+f_{n-2}$ different ways you could have tiled the nx1 checkerboard.

Q.E.D.

If you have ever worked with the Fibonacci numbers before, you know that there are a wealth of different relationships that connect them. Many of these relationships can be proven using algebra, but there's no dignity in that!

Theorem (5.3.9)- If $n \geq 0, f_{n+2}-1=f_0+f_1+f_2+.....+f_n$
Question- How many tilings of an $(n+2)$x1 checkerboard use at least one domino?
Left Side- There are f_{n+2} tilings of the checkboard, but we are eliminating the one tiling that is all squares.
Right Side- We are going to condition on the position of the last domino. What is important to note about this condition is that once we place the "last" domino, there is only ONE way to tile the rest of the boxes in the checkerboard- with squares. With that in mind, we can fix the position of the last domino and count the number of tilings of the boxes that come before it. If the "last" domino covers the first and second boxes, then there are zero boxes that come before the domino, giving us f_0 tilings. If the last domino covers the second and third boxes, then there is only a single box before the domino, and thus f_1 tilings. Now let's say that the last domino covers boxes three and four. Well, then there are two boxes before the domino, and f_2 ways to tile that area. We keep going in this way until the last domino is in position $n+1$ and $n+2$. This yields f_n tilings to cover the n boxes that come before the final domino. Since each positioning of the last domino is a different scenario, we add the results, giving us $f_0+f_1+f_2+.....+f_n$. We have now counted every possible tiling of this checkerboard in two different ways, competing the proof.

■

One final combinatorial proof involving checkerboards and then on to the exercises.

THEOREM (5.4.10)- $f_{2n}=(f_n)^2+(f_{n-1})^2$
Question-How many ways are there to tile a $2n$x1 checkerboard?
Left Side- f_{2n} ways, by our base theorem!
Right Side- Now the tougher part. We have to think about why this relationship is special, or how it differs from our previous proofs. The main difference (that I can

see) is that the size of the checkerboard is twice what we've dealt with up to this point. So I'm going to simply place two nx1 checkerboards end to end so form that $2n$x1 checkerboard. When I place them end to end, I want to keep my eye on the line of demarcation between them. Let's think about how to tile the area around that line of demarcation. There are only two options- we can cover it with a domino, or we can not cover it. If we were to cover it, the domino partitions the $2n$ board into two separate $(n-1)$x1 checkerboards, each which can be tiled in f_{n-1} ways. Since we want to cover the left side of the domino and the right side, we multiply the results together to get $(f_{n-1})^2$ tilings. We can do this OR (that means we are going to add) we can leave the divider alone. If we leave it alone, we are dealing with two separate nx1 checkerboards that do not interact in any way, and thus obtain $(f_n)^2$ more tilings. Over all, we have discovered $(f_n)^2 + (f_{n-1})^2$ total tilings. Having counted the checkerboard in two different ways, our equality must hold, and we have completed the proof.

Q.E.D.

As we have stated before, the problem with combinatorial proofs is often coming up with a proper question that models the relationship you are trying to prove. When working on checkerbaord Fibonacci relationships, it is often helpful to draw a picture and see what is unusual enough to warrant investigation. In the case of Theorem (5.4.10), the divider between our checkerboards was a giveaway on how we must condition our tilings. Also keep in mind that whenever there is an addition sign on one side of the equation, there will be different cases that you need to investigate. If a term is squared, it usually means that the checkerboard is being split into two or more pieces that must be tiled separately. Keep these tips in mind when attempting a combinatorial proof without guidance.

<u>Exercises</u>

1. Prove the following algebraically: $\binom{n-1}{k-1}\binom{n}{k+1}\binom{n+1}{k} = \binom{n-1}{k}\binom{n}{k-1}\binom{n+1}{k+1}$

2. Prove that if n and k are integers with $1 \leq k \leq n$, then $k({}_n\mathrm{C}_k){=}n({}_{n-1}\mathrm{C}_{k-1})$

3. Prove: $({}_n\mathrm{C}_r)({}_r\mathrm{C}_k) = ({}_n\mathrm{C}_k)({}_{n-k}\mathrm{C}_{r-k})$

4. Show that if n and k are positive integers, then: $({}_{n+1}\mathrm{C}_k){=}(n+1)({}_n\mathrm{C}_{k-1})/k$

5. Show that if p is prime and k is a positive integer less than $p-1$, then p divides ${}_p\mathrm{C}_k$

6. Let n be a positive integer. Show that: $({}_{2n}\mathrm{C}_{n+1}) + ({}_{2n}\mathrm{C}_n) = ({}_{2n+2}\mathrm{C}_{n+1})/2$

7. Prove combinatorially: $n! = n(n-1)!$

8. Prove combinatorially for $0 \leq k \leq n$: $n! = \binom{n}{k}k!(n-k)!$

9. Come up with a valid question and then prove combinatorially for $0 \leq k \leq n$: $k\binom{n}{k} = n\binom{n-1}{k-1}$

10. Come up with a valid question and then prove combinatorially for $m, n \geq 0$: $\binom{m+n}{k}$=$\sum_{j=0}^{k}\binom{m}{j}\binom{n}{k-j}$

11. Come up with a good question and prove combinatorially when $0 \leq m \leq k \leq n$: $\binom{n}{k}\binom{k}{m} = \binom{n}{m}\binom{n-m}{k-m}$

12. Use the checkerboard interpretation of the Fibonacci numbers to prove $f_0 + f_2 + f_4 + ... + f_{2n} = f_{2n+1}$

13. Prove combinatorially: $f_{m+n} = (f_m)(f_n) + (f_{m-1})(f_{n-1})$

14. Prove that $\binom{n}{0} + \binom{n-1}{1} + \binom{n-2}{2} + ... = f_n$

We will not be using typical counting methods such as permutations and combinations for the remainder of this chapter. Instead we will focus on a concept that can be used to prove some other combinatorics questions.

(5.4) – Pigeonhole Principle

Q: Say there are eleven dogs to be put in five kennels. Show that there is at least one kennel that houses at least three dogs.
Ans: We will assume the opposite, that there is no kennel that houses three dogs. Then at most, we have five kennels containing two dogs each, for a total of ten dogs. But we said there were 11 dogs, so there is a contradiction. Thus at least one of the kennels contains at least three dogs.

The idea behind this technique is called the **PIGEONHOLE PRINCIPLE**. What we did to solve the previous question might seem obvious, but the uses of Pigeonhole are not always apparent. It is often a very subtle, yet incredibly useful technique.

THEOREM (5.4.1)- If $k+1$ objects are placed in k boxes, then there is at least one box containing more than one object.
Proof- By contradiction: Assume there is no box that contains more than one object. Then there are a total of at most k objects. But we claimed there were $k+1$ objects. CONTRADICTION! Therefore, there exists a box with more than one object.

■

Corollary- A function from a set with at least $k+1$ objects to a set with k objects is not one-to-one.
We will leave the proof as an exercise.

ex: How many people must be in the same room before you can guarantee at lest two of them were born in the same month?
If we want to translate this to a Pigeonhole question, we would call the boxes the months, and the people the objects. If there are 12 boxes, then there would need to be 12+1=13 objects before we could guarantee that two of them fell into the same box.

It is often easier to see the logic behind the Pigeonhole Principle than it is to use the actual math. Another way to think of Pigeonhole questions is as the "worst case scenario". In the previous question, let's say that you were sitting in the room (but don't count as a person, for some reason), and watched as person after person filed in and sat down. You want to leave, but are not allowed to leave until two people in the room with you were born in the same month. Now, if you are anything like me, you think you have horrible luck, and you just know that you will end up being in the room for as long as humanly possible. So what is the worst case scenario? Well, that would be the case of the first person being born in Janurary, the second in February, the third in March, and so on, until you have one person each born in every month. That would make 12 people in total, each born in a different month. Now, when that 13th person walks into the room, no matter what month they were born, will match one of the people already in the room. So the worst case scenario is that it would take 13 people before you could leave the room, and that is the solution.

ex: How many integers must you choose at random before you can guarantee that the difference between two of the numbers is n?
This one is probably confusing because it doesn't give you any numbers to work with. So let's try it for $n = 5$. Now the question is asking how many integers you must choose before you can guarantee the difference between two of them is divisible by 5? As an example, if you were to choose the numbers 1 and 2, their difference is 1, which is not divisible by 5. So the answer is greater than 2 at least. The trick here is to look at the numbers as representatives of congruence classes (mod 5). If you choose two numbers in the same congruence class, their difference is divisible by 5, by the definition of congruence. So the worst case scenario here is that you choose one element from each congruence class. That's 5 numbers; once you choose the next number, two of them will have a difference divisible by 5. So the answer for 5 is 6. And the answer for n is $n + 1$.

THEOREM (5.4.2)- If n objects are placed into k boxes, then there is at least one box containing at least $\lceil \frac{n}{k} \rceil$ objects. This is called the **GENERALIZED PIGEONHOLE PRINCIPLE**.
Proof- Assume no box has $\lceil \frac{n}{k} \rceil$ objects. Then the maximum number of objects a box can contain is $\lceil \frac{n}{k} \rceil - 1$ objects. This means that the maximum number of total objects is $(\lceil \frac{n}{k} \rceil - 1)k$. But $(\lceil \frac{n}{k} \rceil - 1)k \leq ((\frac{n}{k} + 1) - 1)k = n$. This chain tells us that the total number of objects is less than n. CONTRADICTION! So one box must contain at least $\lceil \frac{n}{k} \rceil$ obects.

Q.E.D.

ex: How many cards must be selected from a standard deck of cards to guarantee

that three of the same suit are chosen?
We know that there are four suits, and these are the boxes in the generalized Pigeonhole Principle formula. So $k = 4$, and we want to solve for the minimum possible n. Here's how:
$\lceil \frac{n}{4} \rceil = 3 \rightarrow 2 < \frac{n}{4} \rightarrow 8 < n \rightarrow n = 9$

This last answer meshes with the idea of the worst case scenario. The worst that could happen would be if you chose two each of the four suits, giving you eight total cards. Whatever cards you choose next will be the third in a suit. Now be careful when you answer these questions not to be confused about the wording. Of course you CAN get three of the same suit before you choose the 9th card, but the question asks what is the minimum needed to GUARANTEE you have four of the same suit. It's not asking the minimum possible, it's asking the minimum so that there is no question that you've done it. There IS a difference, and that is at the heart of the Pigeonhole Principle.

Exercises

1. Prove the corollary to Theorem (5.4.1)

2. How many people must be in a room before we can guarantee that five of them were born on the same day of the week?

3. How many integer coordinate points on the xy plane must you randomly choose before you can guarantee that the midpoint between two of those points is made up of only integers?

4. Use Pigeonhole, or any other technique to show that in a room with n people, at least two know the same number of people in that room. Note that if person a knows person b, then person b knows person a.

5. Show that if there are 30 students in a class, then at least two have last names that begin with the same letter.

6. A drawer contains a dozen brown socks and a dozen black socks, all unmatched. A man takes socks out at random in the dark.

   (a) How many socks must he take out to be sure that he has at least two socks of the same color?

   (b) How many socks must he take out to be sure that he has at lest two black socks?

7. A bowl contains 10 red balls and 10 blue balls. A woman selects balls at random without looking at them.

   (a) How many balls must she select to be sure of having at least three balls of the same color?

   (b) How many balls must she select to be sure of having at least three blue balls?

8. Show that among any group of five (not necessarily consecutive) integers, there are two with the same remainder when divided by 4.

9. Let d be a positive integer. Show that among any group of $d+1$ integers there are two with exactly the same remainder when they are divided by d.

10. How many numbers must be selected from the set (1,2,3,4,5,6) to guarantee that at least one pair of these numbers add up to 7?

11. How many numbers must be selected from the set (1,3,5,7,9,11,13,15) to guarantee that at least one pair of these numbers add up to 16?

12. A company stores products in a warehouse. Storage bins in this warehouse are specified by their aisle, location in the aisle, and shelf. There are 50 aisles, 85 horizontal locations in each aisle, and 5 shelves throughout the warehouse. What is the least number of products the company can have so that at least two products must be stored in the same bin?

13. Suppose there are nine students in a math class at a small college.

    (a) Show that the class must have at least five male students or at least five female students.

    (b) Show that the class must have at least three male students or at least seven female students.

14. Show that there are at least six people in California (population: 37 million) with the same three initials who were born on the same day of the year. Assume everyone has three initials.

15. Show that if there are 100,000,000 wage earners in the US who earn less than 1,000,000 dollars, there are two who earned exactly the same amount of money, to the penny, last year.

16. There are five distinct points on the xy coordinate plane. Show that the midpoint of the line joining at least one pair of these points has integer coordinates.