MATH 245 **Exam 1 Notes** **Spring**

1 Logic

Let's go over some basic truth tables:

If p and q are propositions, the conjunction, denoted $p \wedge q$, means p and q.

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

the disjunction, denoted $p \vee q$, means p or q.

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

negation, not p, is denoted $\overline{p}$.

p	$\overline{p}$
T	F
F	T

If p then q, denoted $p \longrightarrow q$, is called the conditional.

p	q	$p \longrightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

The conditional is somewhat counterintuitive so let's examine the following example. Let's say I make the following statement:

"If it stops raining by Saturday, then I will go to the game."

Under what circumstances am I a liar? ONLY if it stops raining and I don't go to the game, that is, $T \longrightarrow F = F$

If it does not stop raining I have not claimed what I will do. Whether I go or not, I have not lied.

p if and only if q, denoted $p \longleftrightarrow q$, is called the biconditional.

p	q	$p \longleftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

DE MORGAN'S LAWS

1. $\overline{p \vee q} \equiv \overline{p} \wedge \overline{q}$
2. $\overline{p \wedge q} \equiv \overline{p} \vee \overline{q}$

You will verify these on the worksheet.

The contrapositive of $p \longrightarrow q$ is denoted $\overline{q} \longrightarrow \overline{p}$. You will verify this as well.

Worksheet for Section 1

1. Evaluate each proposition if $p = F, \quad q = T, \quad r = F$:

   (a) $p \vee q$

   (b) $\overline{p} \vee \overline{(q \wedge r)}$

2. Write the truth table for each:

   (a) $p \wedge \overline{q}$

   (b) $(p \wedge q) \wedge \overline{p}$

   (c) $(p \vee q) \wedge (\overline{p} \vee q) \wedge (p \vee \overline{q}) \wedge (\overline{p} \vee \overline{q})$

3. * Write truth tables to verify BOTH of De Morgan's laws.

4. * Write a truth table to verify the contrapositive.

2 Induction

PRINCIPLE OF MATHEMATICAL INDUCTION

Let $S(n)$ be a statement that is either true or false for each $n \in \mathbb{N}$. Then if

1. **(basis step)** $S(1)$ is true AND
2. **(inductive step)** for each $k \in \mathbb{N}$ if $S(k)$ is true, then $S(k+1)$ is true, then...

$S(n)$ is true $\forall\ n \in \mathbb{N}$

A nice analogy is comparing induction to dominoes. If you were to line up a bunch of dominoes, as long as you know that the first domino gets knocked down (the basis step) AND all the other dominoes are the same distance apart (the inductive step), then you can be sure that no matter how many were lined up, they will all fall.

ex 1

Let $S_n = 1 + 2 + \ldots + n$. Suppose I claim that $S_n = \frac{n(n+1)}{2}$

Really I am claiming a sequence of statements:

$S_1 = \frac{1(2)}{2} = 1$
$S_2 = \frac{2(3)}{2} = 3$
$S_3 = \frac{3(4)}{2} = 6$
$\vdots$

Induction works as follows...

First we need to show that the base case, $n = 1$, is true. We have done that already. Now for the inductive step which says *assuming* S_k *or* S_n *is true, show* S_{k+1} *or* S_{n+1} *is true.* In other words, use S_n to get S_{n+1}. Observe:

by definition, $S_{n+1} = 1 + 2 + 3 + \ldots + n + (n + 1)$, but we get to assume that S_n is true. What is S_n?

Since $S_n = 1 + 2 + \ldots + n$, we have that

$$\begin{aligned} S_{n+1} &= S_n + (n+1) \\ &= \frac{n(n+1)}{2} + (n+1) \\ &= \frac{n(n+1)}{2} + \frac{2(n+1)}{2} \\ &= \frac{(n+1)(n+2)}{2} \\ &= S_{n+1} \end{aligned}$$

■

ex 2

Use induction to show that $n! \geq 2^{n-1}$ for $n = 1, 2, 3, \ldots$

basis step.... Is $1! \geq 2^0$?

We now need to show that $(n + 1)! \geq 2^n$

So,

$$\begin{aligned}(n+1)! &= (n+1)n! \\ &\geq (n+1)2^{n-1} \qquad \text{why?} \\ &\geq (2)2^{n-1} \qquad \text{why?} \\ &= 2^n\end{aligned}$$

■

Worksheet for Section 2

1. Use Induction to show

$$\frac{1}{1(3)} + \frac{1}{3(5)} + \frac{1}{5(7)} + \ \cdots \ + \frac{1}{(2n-1)(2n+1)} = \frac{n}{2n+1}$$

2. Observe that:

$$1 = 1^2$$
$$1 + 3 = 2^2$$
$$1 + 3 + 5 = 3^2$$
$$1 + 3 + 5 + 7 = 4^2$$

   Figure out a general formula and use Induction to show it is correct.

3. * Prove by Induction that $7^n - 4^n$ is a multiple of 3 $\forall\ n \in \mathbb{N}$

3 Set Theory

A set is simply a collection of objects, order doesn't matter.

ex 3

$$A = \{1, 2, 3, 4\} = \{2, 1, 4, 3\} = \{4, 3, 1, 2\} = \dots$$

You can define large sets by listing the properties necessary for membership.

$$B = \{x \Big| x \in \mathbb{Z}^+\}$$

If X is a finite set, $|X|$ is the number of elements in X

$x \in X$ means x is an element of X and $x \notin X$ means x is not an element of X.

$\emptyset = \{\ \}$ is called the null set or the empty set. There are no elements in the null set.

$A = B$ if they have the same elements.

ex 4

If $A = \{2, 4\}$ and $B = \{2, 4, 6, 8\}$, then A is a *subset* of B denoted $A \subset B$

Every set is a subset of itself. If $X \subset Y$ and $X \neq Y$ then X is called a *proper subset*.

The set of ALL subsets of X, denoted $\mathcal{P}(X)$, is the power set of X.

ex 5

If $A = \{a, b, c\}$, then

$$\mathcal{P}(A) = \emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}$$

Note that $|A| = 3$ and $|\mathcal{P}(A)| = 2^3 = 8$

Theorem 1

If $|X| = n$, then $|\mathcal{P}(X)| = 2^n$

Why do you think this is? You will prove this using induction on the worksheet.

Definition 1

The union of two sets is denoted

$$X \cup Y = \{x \Big| x \in X \text{ or } x \in Y\}$$

The intersection of two sets is denoted

$$X \cap Y = \{x \Big| x \in X \text{ and } x \in Y\}$$

The difference of two sets is denoted

$$X - Y = \{x \Big| x \in X \text{ and } x \notin Y\}$$

If $X \cap Y = \emptyset$, then X and Y are *disjoint*.

If a set contains everything it is usually denoted U, the universal set.

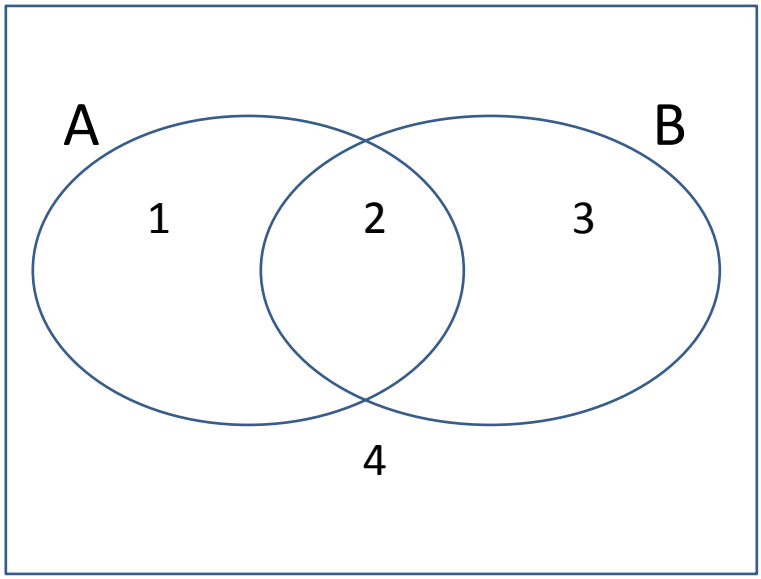
$U - X$ is called the *complement* of X, denoted $\overline{X}$

ex 6

If $U = \{1, 2, 3, \ldots, 10\}$ and $X = \{1, 2\}$, what is $\overline{X}$?

Sometimes we use VENN DIAGRAMS as pictoral views of sets. Rectangles represent the universal set and circles represent subsets.

ex 7



$U =?$ $A =?$ $B =?$

$A \cup B =?$ $A \cap B =?$ $\overline{A} =?$ $A - B =?$

Sets are very well behaved and obey commutativity, associativity, distributive, etc...

DE MORGANS LAWS

1. $(\overline{A \cup B}) = \overline{A} \cap \overline{B}$
2. $(\overline{A \cap B}) = \overline{A} \cup \overline{B}$

You will verify these with Venn Diagrams.

A *partition* of X is when X is divided into non-overlapping subsets.

If S is a partition then it is *pairwise disjoint* and

$\cup S = X$
$\cap S = \emptyset$

Worksheet for Section 3

1. Let $U = \{1, 2, 3, \ldots, 10\}$, $A = \{1, 4, 7, 10\}$, $B = \{1, 2, 3, 4, 5\}$ and $C = \{2, 4, 6, 8\}$. Find:

   (a) $A \cup B$

   (b) $B \cap C$

   (c) $A - B$

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

2. For each condition, what relation must hold between A and B.

   (a) $A \cap B = A$

   (b) $A \cap B = B$

3. Among a group of 165 students, 8 are taking calculus, psychology and French; 33 are taking calculus and French; 20 are taking calculus and psychology; 24 are taking psychology and French; 79 are taking calculus; 83 are taking psychology; and 63 are taking French. Use a Venn diagram to find out how many are taking none of those subjects.

4. * Show that $\mid A \cup B \mid = \mid A \mid + \mid B \mid - \mid A \cap B \mid$

5. * Prove DeMorgan's Laws for sets using Venn Diagrams.

6. * Prove by Induction that if $\mid X \mid \; = n$, then $\mid \mathcal{P}(X) \mid \; = 2^n$

4 Relations

A CARTESIAN PRODUCT, $A \times B$ is an ordered pair

$(a, b) \Big| a \in A$ and $b \in B$.

A *relation*, R, from a set A to a set B is a subset of $A \times B$.

If $(a, b) \in R$, we write aRb and say a is related to b. The set of a's is the domain and the set of b's is the range.

ex 8

Let R be a relation on $X = \{1, 2, 3, 4\}$ defined by $(x, y) \in R$ if $x \leq y$

So, what are the members of R?

$$R = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 3), \ldots, (4, 4)\}$$

Definition 2

A relation is reflexive if $(x, x) \in R \quad \forall\, x$

A relation is symmetric if $(x, y) \in R$ then $(y, x) \in R \quad \forall\, x, y$

A relation is transitive if $(x, y) \in R$ and $(y, z) \in R$ then $(x, z) \in R \quad \forall\, x, y, z$

Looking back at **ex 8**, is R reflexive? Symmetric? Transitive?

Theorem 2

Let S be a partition of a set X. Define xRy to mean that for some set in S, both x and y belong to that set. The R is reflexive, symmetric and transitive.

A relation that is reflexive, symmetric and transitive is called an *equivalence relation*

ex 9

Consider the following relation:

$$R = \{(1,1), (1,3), (1,5), (2,2), (2,4), (3,1), (3,3), (3,5), (4,2), (4,4), (5,1), (5,3), (5,5)\}$$

Is R an equivalence relation?

What are the equivalence classes?

Worksheet for Section 4

1. Let $X = \{1, 2, 3, 4, 5\}$. Define the relation R by the rule $(x, y) \epsilon\ R\ if\ 3\ divides\ x - y$. List the elements of R.
2. Repeat the previous exercise if the rule is $(x, y) \epsilon\ R\ if\ x + y \leq 6$.
3. * Determine if the following relations are reflexive, transitive and symmetric.
   (a) $(x, y) \epsilon\ R\ if\ x = y$.
   (b) $(x, y) \epsilon\ R\ if\ x < y$.
4. * Let $X = \{1, 2, 3, 4, 5\}$. Determine if the following relation is an equivalence relation. If it is, list the equivalence classes.

$$\{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (1, 3), (3, 1)\}$$

5 Functions

Traditionally functions have been described by a formula, now we will move to a more general idea.

In a correspondence between sets, a given element in the first set can NOT correspond to two different elements in the second set.

A function is really a special kind of relation.

Definition 3

If A and B are sets, a *function* between A and B is a non-empty relation such that if $(a, b) \in f$ and $(a, c) \in f$ then $b = c$.
The notation for a function from A to B is $f : A \longrightarrow B$

$dom\ f$ is the set of all the first elements.

$range\ f$ is the set of all the second elements.

the set A is the domain, HOWEVER, the set B is the co-domain which is NOT necessarily the $range\ f$.

ex 10

Let $A = \{1, 2, 3\}$ and $B = \{2, 4, 6, 8\}$

Which of the following are functions?

1. $\{(1, 2), (2, 6), (3, 4), (2, 8)\}$
2. $\{(1, 6), (2, 6), (3, 2)\}$
3. $\{(1, 8), (2, 2), (3, 4)\}$

Note that for (2) $f : A \longrightarrow B$ is a function. Suppose that $C = \mathbb{R}$ and $D = \{2, 6\}$.

Is $f : A \longrightarrow C$ a function?

Is $f : A \longrightarrow D$ a function?

Is there anything interesting or unique about $f : A \longrightarrow D$?

Definition 4

A function $f : A \longrightarrow B$ is *surjective* or *onto* if $B = range\ f$.

A function can always be "forced" to be surjective. How?

Definition 5

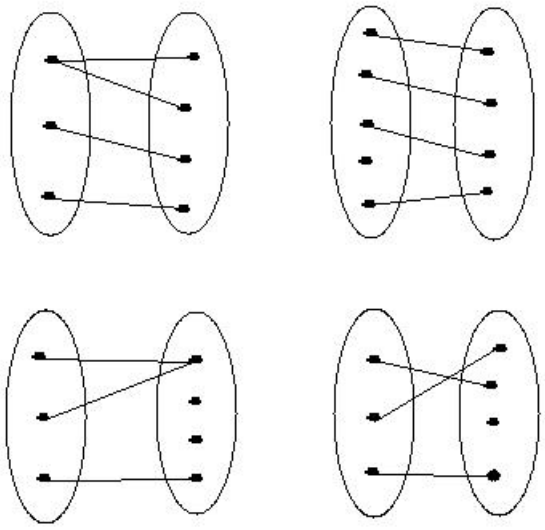
A function $f : A \longrightarrow B$ is *injective* or *one to one* if $\forall\ a, b \in A,\ f(a) = f(b) \Longrightarrow a = b$.

Definition 6

A function $f : A \longrightarrow B$ is a *bijection* if it is BOTH surjective and injective.

Worksheet for Section 5

1. Consider the pictures below. Classify each as being a function, and if so, as surjective, injective or bijective.



2. * Given $f : A \longmapsto B$ and $y \in B$, under what conditions on f can we assert that there exists an x in A such that $f(x) = y$?

3. * Given $f : A \longmapsto B$ and $y \in B$, under what conditions on f can we assert that there exists a unique x in A such that $f(x) = y$?

4. * For the following function, $f(x) = x^2 + 2$, $f : \mathbb{R} \longmapsto \mathbb{R}$, find:

   (a) the codomain

   (b) the range

   (c) the domain

   (d) Is f injective?

   (e) Is f surjective?

6 Cardinality

Cardinality refers to the "size" of a set.

If $S = \{a, b\}$ and $T = \{1, 2, 3\}$ it is fairly intuitive that the set T is "larger".

How should we compare $\mathbb{N}$ and $\mathbb{R}$? This is not so intuitive. First, some definitions.

Definition 7

Two sets, S and T are *equinumerous*, denoted $S \sim T$, if there exists a bijection from S to T.

Definition 8

If $S = \emptyset$ or $\exists\ n \in \mathbb{N}$ and a bijection $f : \{1, 2, 3, \ldots, n\} \longrightarrow S$, then S is <u>finite</u>. If S is not finite then it is <u>infinite</u>.

We will abbreviate the set $\{1, 2, 3, \ldots, n\}$ by I_n

Definition 9

The cardinal number of I_n is n and if $S \sim I_n$, S has n elements.

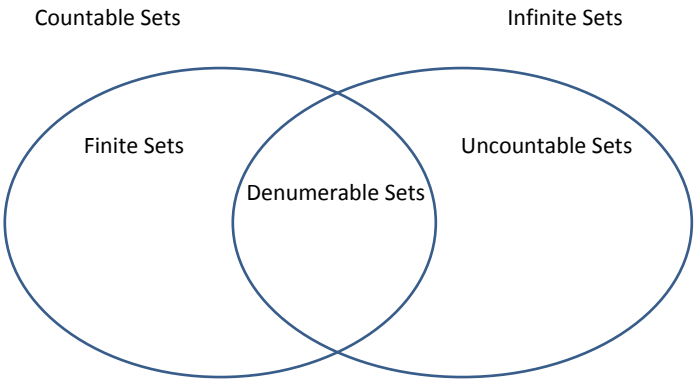
If a cardinal number is not finite, it is called <u>transfinite</u>

Definition 10

A set S is *denumerable* if $\exists$ a bijection $f : \mathbb{N} \longrightarrow S$. If S is finite or denumerable, it is called countable. If it is not countable, it is called uncountable.

The cardinal number of a denumerable set is $\aleph_0$.

A set is denumerable $\iff$ it is equinumerous with $\mathbb{N}$



Not every infinite set has $\aleph_0$ as its cardinal number!

There are different sizes of infinity!

ex 11

Which set do you think is larger, $\mathbb{N}$ or $E =$ the set of even natural numbers?

What is half of $\aleph_0$?

If I claim they are actually the same size, how could I validate that claim? Find the bijection!

Theorem 3

If S is countable and $T \subset S$, then T is countable.

Theorem 4

The union of countable sets is also countable.

Theorem 5

$\mathbb{R}$ is uncountable.

The proof is sometimes referred to as Cantor's diagonal method.

proof:

It suffices to show that $J = (0, 1)$ is uncountable. If J were countable, then you could list its members. That is,

$$J = \{x_1, x_2, x_3, \ldots\} = \{x_n \Big| n \in \mathbb{N}\}$$

Now each element in J has an infinite decimal expansion, so

$$\begin{aligned} x_1 &= 0.a_{11}a_{12}a_{13}\ldots \\ x_2 &= 0.a_{21}a_{22}a_{23}\ldots \\ x_3 &= 0.a_{31}a_{32}a_{33}\ldots \\ x_4 &= 0.a_{41}a_{42}a_{43}\ldots \\ &\vdots \end{aligned}$$

$$\text{where} \quad a_{ij} \in \{0, 1, 2, 3, \ldots, 9\}$$

Let's construct a a number $y = b_1b_2b_3\ldots$ such that

$$b_n = \begin{cases} 2 \;\; if \;\; a_{nn} \neq 2 \\ 3 \;\; if \;\; a_{nn} = 2 \end{cases}$$

So clearly $y \in J$ but it is not one of the x_n's since it differs from x_n in the nth decimal place. This contradicts our assumption, therefore J is uncountable.

The cardinal number of $\mathbb{R}$ is denoted c.

Since $\mathbb{N}$ is countable and $\mathbb{R}$ is uncountable, we have

$$\aleph_0 < c$$

These are unequal transfinite cardinals! Are there others?

Theorem 6

For any set S, $|S| < |\mathcal{P}(S)|$

So, you can get an infinite sequence of transfinite cardinals,

$$\aleph_0 = |\mathbb{N}| < |\mathcal{P}(\mathbb{N})| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))| < \ldots$$

Does there exist a cardinal number λ, such that $\aleph_0 < \lambda < c$?

This conjecture is the continuum hypothesis. Unfortunately it has been shown that the continuum hypothesis can neither be proved nor disproved.

Worksheet for Section 6

1. Find a bijection, $f : \mathbb{N} \longmapsto \mathbb{Z}$, thereby showing that the set $\mathbb{Z}$ of all integers is also denumerable.

2. * Show that the set of rational numbers, $\mathbb{Q}$, is countable.

3. * Show that the set of irrational numbers is uncountable.

7 Number Theory 1

Basically, number theory is the study of the integers.

some unanswered questions:

Fermats Last Theorem

You should be familiar with the integer solutions to $x^2 + y^2 = z^2$, how about integer solutions to $x^n + y^n = z^n$ for $n > 2$?

This was solved in 1995.

Twin Prime Conjecture

A prime number is a number divisible by itself and 1 only. There are many examples of pairs of primes that differ by 2, for example $(3, 5), (5, 7), (11, 13), (17, 19)$.

Are there an infinite number of these?

Goldbach Conjecture

It seems possible to write every even number greater than 2 as the sum of two primes. Can this always be done?

$$\begin{aligned} 4 &= 2 + 2 \\ 6 &= 3 + 3 \\ 8 &= 3 + 5 \\ 10 &= 3 + 7 \\ &\vdots \end{aligned}$$

An integer is *perfect* if it is the sum of its positive divisors other than itself. For example, 6 is perfect since $1+2+3=6$. Are there infinitely many?

Number theory is not only intrinsically interesting, but as you can see it is one of the rare disciplines in math where the unanswered questions are very easy to understand. In most areas, quite a bit of study is required just to understand the problems.

Definition 11

We say that a divides b, denoted $a \big| b$, when $\frac{b}{a}$ is an integer. Also, b is a multiple of a. If not, $a \nmid b$.

ex 12

$3 \big| 6$, $-3 \big| 6$, $2 \nmid 5$

Definition 12

d is the *greatest common divisor*, (gcd), of a and b when d is the largest integer dividing both a and b. It is denoted $d = (a, b)$

ex 13

The divisors of 4 are 1,-1,2,-2,4,-4
The divisors of 2 are 1,-1,2,-1

The common divisors are 1,-1,2,-2 $\implies$ $(4, 2) = 2$

Definition 13

m is the *least common multiple*, (lcm), of a and b when m is the smallest positive integer that is a multiple of both a and b. It is denoted $m = [a, b]$

ex 14

The multiples of 4 are $4, 8, 12, 16, 20, 24, \ldots$
The multiples of 6 are $6, 12, 18, 24, 30, \ldots$

The common multiples are $12, 24, \ldots$ $\implies$ $[4, 6] = 12$

SOME THEOREMS:

Theorem 7

If $a \big| b$ and $b \big| c$ then $a \big| c$

PROOF:

by definition of $a \big| b$, $\frac{b}{a}$ is an integer as well as $\frac{c}{b}$
So,

$$\frac{b}{a} \cdot \frac{c}{b} = \frac{c}{a} \implies a \big| c \qquad \blacksquare$$

Theorem 8

If $a \mid b$ and $a \mid c$ then $a \mid bx + cy \ \ \forall\ x, y \in \mathbb{Z}$

PROOF:

$a \mid b \implies \exists r \in \mathbb{Z}$ such that $b = ra$

$a \mid c \implies \exists s \in \mathbb{Z}$ such that $c = sa$

So,

$$bx + cy = (ra)x + (sa)y = a(rx + sy) \implies a \mid bx + cy$$

■

Theorem 9

DIVISION ALGORITHM
Suppose that $a, b \in \mathbb{Z},\ a > 0$

then $\exists$ unique integers q and r, $0 \leq r < a$ such that $b = aq + r$

q is the quotient and r is the remainder.

ex 15

If $a = 7$ and $b = 592$, then $q = 84$ and $r = 4$ since $592 = 7 \cdot 84 + 4$

We will return to this later...

Theorem 10

If $a, b \in \mathbb{Z}^+$ then $(a, b)[a, b] = ab$

Worksheet for Section 7

1. Find $(51, 34)$ and $[51, 34]$.
2. Find all $d > 0$ such that $18 \mid d$ and $d \mid 216$.
3. For what integers a is $1 \mid a$ true?
4. For what integers a is $a \mid 0$ true?
5. Find q and r by the Division Algorithm if $a = 13$ and $b = 380$
6. * Prove that if $d \mid a$, $d \mid b$ and $d \mid c$, and if x, y and z are any integers, then d divides $ax + by + cz$.
7. * Show why $ab/(a, b)$ must be an integer whenever (a, b) is defined.
8. * Show that $[a, b]$ is defined if and only if neither a nor b is 0.

8 Number Theory 2

THE EUCLIDEAN ALGORITHM

So far, there is no easy way to find (a, b). A list is rather tedious.

Let's look at the Division Algorithm again...

ex 16

Find $(504, 123)$

Observe that:

$$504 = 123 \cdot 4 + 12$$
$$123 = 12 \cdot 10 + 3$$
$$12 = 3 \cdot 4 + 0$$

the gcd is the last **nonzero** remainder, that is

$$(504, 123) = (12, 123) \implies (12, 123) = (3, 12) \text{ thus } (504, 123) = 3$$

ex 17

Compute $(158, 188)$

$$\textcircled{1}\quad 188 = 158 \cdot 1 + 30$$
$$\textcircled{2}\quad 158 = 30 \cdot 5 + 8$$
$$\textcircled{3}\quad 30 = 8 \cdot 3 + 6$$
$$\textcircled{4}\quad 8 = 6 \cdot 1 + 2$$
$$6 = 2 \cdot 3 + 0$$

thus $(158, 188) = 2$

Let's reverse this process to write (a, b) in the form $ax + by$

$$
\begin{aligned}
&\textcircled{4} \quad 2 = 8 - 6 \cdot 1 \\
&\textcircled{3} \quad = 8 - (30 - 8 \cdot 3) \cdot 1 = -30 + 8 \cdot 4 \\
&\textcircled{2} \quad = -30 + (158 - 30 \cdot 5)4 = 158 \cdot 4 - 30 \cdot 21 \\
&\textcircled{1} \quad = 158 \cdot 4 - (188 - 158)21 = -188 \cdot 21 + 158 \cdot 25
\end{aligned}
$$

thus $(158, 188) = 158x + 188y$ for $x = 25$ and $y = -21$

If either a or b is negative, then just calculate using $|a|$ and $|b|$ and insert the correct signs at the end of the problem.

Theorem 11

Given $a, b, c \in \mathbb{Z}$ with $a, b \neq 0$ $\exists\ x, y$ such that $ax + by = c \iff (a, b) \mid c$

Corollary

$\exists\ x, y \in \mathbb{Z}$ such that $ax + by = 1 \iff (a, b) = 1$

If $(a, b) = 1$, we say that a and b are *relatively prime*

If $(a, b) \mid c$ then the Euclidean Algorithm gives us a solution to $ax + by = c$

ex 18

Consider $9x + 24y = 15$

So $(9, 24)$ is

$$\begin{aligned} 24 &= 9 \cdot 2 + 6 \\ 9 &= 6 \cdot 1 + 3 \\ 6 &= 3 \cdot 2 + 0 \end{aligned}$$

Since $(9, 24) = 3$ and $3 \mid 15$, there exists a solution. In fact,

$$3 = 9 - 6 \cdot 1 = 9 - (24 - 9 \cdot 2)1 = 9 \cdot 3 - 24 \cdot 1$$

so

$$15 = 3 \cdot 5 = (9 \cdot 3 - 24 \cdot 1)5 = 9 \cdot 15 - 24 \cdot 5$$

thus $x = 15, y = -5$ is a solution. There are others. In fact...

Theorem 12

Let x_0, y_0 be a particular solution to $ax + by = c$. Then all solutions are of the following form:

$$x \;=\; x_0 + \frac{b}{d} \cdot t \qquad \text{and} \qquad y \;=\; y_0 - \frac{a}{d} \cdot t$$

as t runs through the integers and $(a, b) = d$

from **ex 18** $9x + 24y = 15$, $x_0 = 15, y_0 = -5$ and $(9, 24) = 3$

So

$$x \;=\; 15 + \frac{24}{3} \cdot t = 15 + 8t \;\text{ and}$$

$$y \;=\; -5 - \frac{9}{3} \cdot t = -5 - 3t$$

Worksheet for Section 8

1. Find (a, b) using the Euclidean Algorithm and solve backwards to get an x and y such that $ax + by = (a, b)$ for $a = 217$, $b = 341$.
2. Use the information from 1 to solve $217x + 341y = 62$.
3. Why is $4x + 6y = 25$ unsolvable?
4. Does $21x - 14y = 10000$ have a solution? Why or why not?
5. Find all solutions to $5x + 6y = 100$.
6. * Prove that if v is a linear combination of w and x and if w and x are each linear combinations of y and z then v is a linear combination of y and z.
7. * Farmer A owes Farmer B \$10. Neither has any cash, but Farmer A has 14 cows that are valued at \$185 each. Farmer A suggests paying his debt in cows with Farmer B making change by giving A some pigs valued at \$110 each. Is this possible, and how?

9 Number Theory 3

Definition 14

A positive integer is *prime* when it has exactly 2 positive divisors. If a number has more than two positive divisors it is called *composite*. By definition, 1 is neither.

Theorem 13

Any number n, $n > 1$, can be written as a product of primes.

Definition 15

Let $d(n)$ denote the number of positive divisors of n.

Theorem 14

If an integer n, $n > 1$, has no prime divisors less than or equal to $\sqrt{n}$, then n is prime.

SIEVE OF ERATOSTHENES

Given a list of integers, circle the first prime, then cross out all of its multiples. Then circle the second prime and cross out all of its multiples, etc... Any integers that remain are prime.

ex 19

Let's find all the primes less than 100.

from the previous theorem, we only need to cross out the multiples of those primes ≤ 10 since $\sqrt{100} = 10$

in other words, first circle 2 and then cross out all of its multiples, then circle the next prime, 3, and cross out all of its multiples. Continue this process for 5 and 7 and whatever integers remain are primes.

Theorem 15

The number of primes is infinite.

there are a number of different proofs for this theorem, we will go over Euclid's proof.

For the sake of contradiction, (FTSOC), suppose there are a finite number of primes. Let's label them:

$$p_1, p_2, p_3, \ldots, p_k$$

Let's create a new number, Q, by multiplying all of the primes together and adding 1. That is,

$$Q = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_k + 1$$

Now, either Q is prime, in which case we are done (Why?) or Q has a prime factor. If Q has a prime factor then it must differ from $p_1, p_2, p_3, \ldots, p_k$ since none of those can divide Q. This again contradicts the assumption that $p_1, p_2, p_3, \ldots, p_k$ are all of the primes.

■

Theorem 16

If $n = p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$ where the p's are distinct primes, then

$$d(n) = (k_1 + 1)(k_2 + 1) \dots (k_t + 1)$$

ex 20

$$d(120) = d(2^3 3^1 5^1) = 4 \cdot 2 \cdot 2 = 16$$

Why does this work? Go through the options...

Theorem 17

If a and b are relatively prime, then

$$d(ab) = d(a)d(b)$$

Worksheet for Section 9

1. Use the Sieve of Eratosthenes to find all the primes between 1000 and 1025.
2. Find $d(900)$.
3. * Show that if $d \mid a$ and $e \mid b$, then $de \mid ab$.
4. * Prove that if $(a, b) > 1$ then $d(ab) < d(a)d(b)$.
5. * Show that if $d(n)$ is prime, then n is a power of a prime.