MATH 145 LECTURE NOTES

Zhongwei Zhao

My Lecture Notes for MATH 145 2016 Fall

December 2016

Lecture 1, Sept. 9

Course Orientation and Organization About the Professor Stephen New
MC 5419
Ext 35554
Email: snew@uwaterloo.ca
Website: www.math.uwaterloo.ca/ snew
Office Hour: MTWF 11:30-12:30

Recommended Textbook

- An Introduction to Mathematical Thinking by Will J. Gilbert, Scott A. Vanstone
- Lecture Notes: Integers, Polynomials and Finite Fields by K. Davidson

Some Paradoxes There are lots of paradoxes in English, such as "This statement is false".

There are also some paradoxes in Mathematical world.

Russell's Paradox Let X be the set of all sets. Let $S = \{A \in X | A \notin A\}$. Is $S \in S$?

Some Question To avoid such paradoxes, some question was raised.

1. What is an allowable mathematical object?
2. What is an allowable mathematical statement?
3. What is an allowable mathematical proof?

Mathematical Object Essentially all mathematical objects are (mathematical) sets. In math, a set is a certain specific kind of collection whose elements are sets. Not all collection of sets are called sets. For a collection to be a set, it must be constructable using specific rules. These rules are called the ZFC axioms of set theory (or the Zermelo–Fraenkel axioms along with the Axiom of Choice)

These axioms include (imply) the following:

- Empty Set: there exist a set, denoted by $\emptyset$, with no elements.
- Equality: two sets are equal when they have the same elements. $A = B$ when for every set x, $x \in A \iff x \in B$
- Pair Axiom: if A and B are sets then so is $\{A, B\}$
- Union Axiom: if S is a set of sets then $\cup_S = \{x | x \in A \text{ for some } A \in S\}$. If A and B are sets, then so is $\{A, B\}$ hence so is $A \cup B = \cup_{\{A,B\}}$

Lecture 2, Sept. 12

Mathematics Contest Big Contests

- Small C
- Big E/Special K
- Putnam
- Bernoulli Trials

Students Run

- Integration Bee
- over 6000

Others

- Recreational Problem Sessions

ZFC Axioms

- Empty Set: there exist a set, denoted by $\emptyset$, with no elements.
- Equality: two sets are equal when they have the same elements. $A = B$ when for every set x, $x \in A \iff x \in B$
- Pair Axiom: if A and B are sets then so is $\{A, B\}$. In particular, taking $A = B$ shows that $\{A\}$ is a set.
- Union Axiom: if S is a set of sets then $\cup_S = \bigcup_{A \in S} A = \{x \mid x \in A \text{ for some } A \in S\}$. If A and B are sets, then so is $\{A, B\}$ hence so is $A \cup B = \cup_{\{A,B\}}$
- Power Set Axiom: if A is a set, then so is its Power Set $P(A)$. $P(A) = \{X \mid X \subseteq A\}$. In particular, $\emptyset \subseteq X$, $X \subseteq X$
- Axiom of Infinity: if we define

$$\begin{aligned} 0 &= \emptyset \\ 1 &= \{0\} = \{\emptyset\} \\ 2 &= \{0, 1\} = \{\emptyset, \{\emptyset\}\} \\ 3 &= \{0, 1, 2\} = \{\emptyset, \{\emptyset, \{\emptyset\}\}\} \\ &\vdots \\ n + 1 &= n \cup \{n\} \end{aligned}$$

  Then $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ is a set (called the set of natural numbers)

Lecture 3, Sept. 13

Women in Math Tue Sept. 13
4:30-6:00
DC 1301

ZFC Axioms

- Empty Set: there exist a set, denoted by $\emptyset$, with no elements.
- Equality: two sets are equal when they have the same elements. $A = B$ when for every set x, $x \in A \iff x \in B$
- Pair Axiom: if A and B are sets then so is $\{A, B\}$. In particular, taking $A = B$ shows that $\{A\}$ is a set.
- Union Axiom: if S is a set of sets then $\cup_S = \bigcup_{A \in S} A = \{x \mid x \in A \text{ for some } A \in S\}$. If A and B are sets, then so is $\{A, B\}$ hence so is $A \cup B = \cup_{\{A,B\}}$
- Power Set Axiom: if A is a set, then so is its Power Set $P(A)$. $P(A) = \{X \mid X \subseteq A\}$. In particular, $\emptyset \subseteq X$, $X \subseteq X$
- Axiom of Infinity: if we define

$$\begin{aligned} 0 &= \emptyset \\ 1 &= \{0\} = \{\emptyset\} \\ 2 &= \{0, 1\} = \{\emptyset, \{\emptyset\}\} \\ 3 &= \{0, 1, 2\} = \{\emptyset, \{\emptyset, \{\emptyset\}\}\} \\ &\vdots \\ n + 1 &= n \cup \{n\} \end{aligned}$$

  Then $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ is a set (called the set of natural numbers)

- Specification Axioms: if A is a set, and $F(x)$ is a mathematical statement about an unknown set x, then $\{x \in A \mid F(x) \text{ is true }\}$ is a set.

  Examples:

$$\{x \in \mathbb{N} \mid x \text{ is even }\} = \{0, 2, 4, 6, \dots\}$$

$$A \cap B = \{x \in A \cup B \mid x \in A \text{ and } x \in B\}$$

- Replacement Axioms: if A is a set and $F(x, y)$ is a mathematical statement about unknown sets x and y with the property that for every $x \in A$ there is a unique set y such that the statement is true, and if we denote this unique set y by $y = F(x)$, then $\{F(x) \mid x \in A\}$ is a set.
- Axiom of Choice: if S is a set of non-empty sets then there exists a function $F \colon S \to U_S$ which is called a choice function for S such that

$$F(A) \in A \quad \forall A \in S$$

Things that are sets

3.1 Example.

$$A \cup B = \{x \mid x \in A \text{ or } x \in B\}$$
$$A \cap B = \{x \in A \cup B \mid x \in A \text{ and } x \in B\}$$
$$A \backslash B = \{x \in A \mid x \notin B\}$$
$$A \times B = \{(x, y) \mid x \in A, x \in B\}$$
$$A^2 = A \times A$$

One way to define ordered pairs

$$(x, y) = \{\{x\}, \{x, y\}\}$$
$$x \in A, y \in B \therefore x, y \in A \cup B$$
$$\{x\}, \{x, y\} \in P(A \cup B)$$
$$(x, y) = \{\{x\}, \{x, y\}\} \subseteq P(A \cup B)$$
$$(x, y) \in P(P(A \cup B))$$
$$\therefore A \times B = \{(x, y) \in P(P(A \cup B)) \mid x \in A \text{ and } y \in B\}$$

function When A and B are sets, a function from A yo B is a subset $F \subseteq A \times B$ with the property that for every $x \in A$ there exists a unique $y \in B$ such that $(x, y) \in F$

When F is a function from A to B we write

$$F \colon A \to B$$

and for $x \in A$ and $y \in B$ we write $y = F(x)$ to indicate that $(x, y) \in F \subseteq A \times B$

Sequence A sequence $a_0, a_1, a_2, \ldots$ of natural numbers is a function $a \colon \mathbb{N} \to \mathbb{N}$ and we write $a(k)$ as a_k

Less than the relation $<$ on $\mathbb{Z}$ is a subset $<\subseteq \mathbb{Z}^2$ and we write $x < y$ when $(x, y) \in <$

We can use the ZFC Axioms to define and construct

- $\mathbb{Z}$: the set of integers
- $\mathbb{Q}$: the set of rationals
- $\mathbb{R}$: the set of real numbers
- $+, \times$: operations
- $<, >$: relations

Lecture 4, Sept. 14

Class

4.1 Definition. A class is a collection of sets of the form

$$\{x \mid F(x) \text{ is true } \}$$

Where $F(x)$ is a mathematical statement about an unknown set x.

4.2 Example. The collection of all sets is the class $\{x \mid x = x\}$

4.3 Example. If A is a set then $A = \{x \mid x \in A\}$ which is also a class

Mathematical Statement

4.4 Definition. In the languages of Propositional logic we use symbols from the symbol set

$$\{\neg, \wedge, \vee, \rightarrow, \leftrightarrow, (,)\}$$

together with propositional variable symbols such as $P, Q, R, \ldots$

The variable symbols are intended to represent mathematical statements which are either true or false.

In propositional logic, a formula is a non-empty, finite string of symbols (from the above set of symbols) which can be obtained by applying the following rules.

1. Every propositional variable is a formula.
2. If F is a formula, then so is the string $\neg F$.
3. If F and G are formulas then so is each of the following strings
   - $(F \vee G)$
   - $(F \wedge G)$
   - $(F \rightarrow G)$
   - $(F \leftrightarrow G)$

A derivation for a formula F is a list of formulas

$$F_1, F_2, F_3, \ldots$$

with $F = F_k$ for some index k and for each index l, either F_l is a propositional variable, or F_l is equal to $F_l = \neg F_i$ for some $i < l$, or $F_l = (F_i * F_j)$ for some $i, j < l$ and for some symbol $* \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$

4.5 Example.

$$(\neg(\neg P \rightarrow Q) \leftrightarrow (R \vee \neg S))$$

is a formula and one possible derivation, with justification on each line, is as follows

1. P

2. Q
3. R
4. S
5. $\neg P$
6. $(\neg P \to Q)$
7. $\neg S$
8. $R \vee \neg S$
9. $\neg(\neg P \to Q)$
10. $(\neg(\neg P \to Q) \leftrightarrow (R \vee \neg S))$

4.6 Definition. An **assignment** of truth-values to the propositional variables is a function $\alpha\colon \{P, Q, R \dots\} \to \{0, 1\}$

For a propositional variable X when $\alpha(X) = 1$ we say $X$is true under α and when $\alpha(X) = 0$ we say X is false under α

Given an assignment $\alpha\colon$ {propositional variables} $\to 0, 1$ we extend α to a function $\alpha\colon$ {formulas} $\to 0, 1$ by defining $\alpha(F)$ for all formulas F recursively as follows:

When $F = X$ where X is a propositional variable symbol, the value of $\alpha(X)$is already known

When $F = \neg G$ where G is a formula, define $\alpha(F)$ according to the following table

G	$\neg G$
1	0
0	1

When $F = (G * H)$ where G and H are formulas and where $* \in \{\wedge, \vee, \to, \leftrightarrow\}$

we define $\alpha(F)$ according to the following table

G	H	$G \wedge H$	$G \vee H$	$G \to H$	$G \leftrightarrow H$
1	1	1	1	1	1
1	0	0	1	0	0
0	1	0	1	1	0
0	0	0	0	1	1

Lecture 5, Sept. 16

Mathematical Statement Given a formula F and an assignment α, (that is give the values of $\alpha(P), \alpha(Q), \alpha(R), \dots$), we can calculate $\alpha(F)$ by making a derivation $F_1, F_2, F_3, \dots, F_l$ for F then calculate the values $\alpha(F_1), \alpha(F_2), \dots$ one at a time.

5.1 Example. Let F be the formula $F = (\neg(P \leftrightarrow R) \vee (Q \to \neg R))$ and let α be an assignment then with $\alpha(P) = 0$, $\alpha(Q) = 1$ and $\alpha(R) = 0$. Find $\alpha(F)$.

We make a derivation $F_1, F_2, F_3, \dots, F_l$ for F and calculate the values $\alpha(F_k)$

P	Q	R	$P \leftrightarrow R$	$\neg(P \leftrightarrow R)$	$\neg R$	$Q \to \neg R$	F
0	1	0	1	0	1	1	0

Truth Table

5.2 Definition. For variable symbols $P_1, P_2, \dots, P_n$, an assignment on $(P_1, P_2, \dots, P_n)$ is a function

$$\alpha \colon \{P_1, P_2, \dots, P_n\} \to \{0, 1\}$$

For a formula F which only involves the variable symbols in $\{P_1, P_2, \dots, P_n\}$, a truth table for F on $(P_1, P_2, \dots, P_n)$ is a table whose top header row is a derivation $F_1, F_2, F_3, \dots, F_l$ for F with $F_i = P_i$ for $1 \leq i \leq n$, and under the header row there are 2^n rows which correspond to the 2^n assignments on $(P_1, P_2, \dots, P_n)$. For each assignment $\alpha \colon \{P_1, P_2, \dots, P_n\} \to \{0, 1\}$ there is a row of the form $\alpha(F_1), \alpha(F_2), \dots, \alpha(F_n)$ and the rows are listed in order such that in the first n columns, the rows $\alpha(F_1), \alpha(F_2), \dots, \alpha(F_n)$ (that is $\alpha(P_1), \alpha(P_2), \dots, \alpha(P_n)$) list the 2^n binary numbers from $111\dots1$ at the top, in order, down to $000\dots0$ at the bottom.

5.3 Example. Make a truth table for the formula

$$F = P \leftrightarrow (Q \wedge \neg(R \to P))$$

P	Q	R	$R \to$P	$\neg(R \to P)$	$Q \wedge \neg(R \to P)$	F
1	1	1	1	0	0	0
1	1	0	1	0	0	0
1	0	1	1	0	0	0
1	0	0	1	0	0	0
0	1	1	0	1	1	0
0	1	0	1	0	0	1
0	0	1	0	1	0	1
0	0	0	1	0	0	1

Tautology Let F and G be formula and let S be a set of formulas

5.4 Definition. We say that F is a tautology, and we write $\vDash F$, when $\alpha(F) = 1$ for every assignment α

We say that F is a contradiction when $\alpha(F) = 0$ for every assignment α, or equivalently when $\vDash \neg F$

We say that F is equivalent to G, and we write $F \equiv G$ when $\alpha(F) = \alpha(G)$ for every assignment α

We say that argument "S therefore G" is valid, or that "S induces G" or that "G is a consequence of S", when for every assignment α for which $\alpha(F) = 1$ for every $F \in S$ we have $\alpha(G) = 1$.

When $S = \{F_1, F_2, \ldots, F_n\}$ we have $S \vDash G$ is equivalent to $\{((F_1 \wedge F_2) \wedge \cdots \wedge F_n)\} \vDash G$ which is equivalent to $\vDash (((F_1 \wedge F_2) \wedge \cdots \wedge F_n) \rightarrow G)$

Lecture 6, Sept. 19

Tautology

Let F and G be formula and let S be a set of formulas

Notation. We say that F is a tautology, and we write $\vDash F$, when $\alpha(F) = 1$ for every assignment α

We say that F is a contradiction when $\alpha(F) = 0$ for every assignment α, or equivalently when $\vDash \neg F$

We say that F is equivalent to G, and we write $F \equiv G$ when $\alpha(F) = \alpha(G)$ for every assignment α

We say that argument "S therefore G" is valid, or that "S induces G" or that "G is a consequence of S", when for every assignment α for which $\alpha(F) = 1$ for every $F \in S$ we have $\alpha(G) = 1$.

When $S = \{F_1, F_2, \ldots, F_n\}$ we have $S \vDash G$ is equivalent to $\{((F_1 \wedge F_2) \wedge \cdots \wedge F_n)\} \vDash G$ which is equivalent to $\vDash (((F_1 \wedge F_2) \wedge \cdots \wedge F_n) \to G)$

When we consider an argument "S therefore G", the formula in S are called the premises for the hypothesis or the assumption and the formula G is called the conclusion of the argument.

Here are some examples of tautology.

1. $\vDash F \vee \neg F$
2. $\vDash P \to P$
3. $\vDash P \leftrightarrow P$
4. $\vDash \neg(P \wedge \neg P)$
5. $\vDash \neg P \to (P \to Q)$
6. $\vDash Q \to (P \to Q)$

Here are some truth equivalences

1. $P \equiv P$
2. $P \equiv \neg\neg P$
3. $P \vee Q \equiv Q \vee P$
4. $P \wedge Q \equiv Q \wedge P$
5. $P \leftrightarrow Q \equiv Q \leftrightarrow P$
6. $(P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R)$
7. $(P \vee Q) \vee R \equiv P \vee (Q \vee R)$
8. $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$
9. $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$

Here are some valid argument

1. $\{P\} \vDash P$
2. $\{P \wedge Q\} \vDash P$
3. $\{P \wedge Q\} \vDash Q$
4. $P \vDash \{P \wedge Q\}$
5. $Q \vDash \{P \wedge Q\}$
6. $\{\neg P\} \vDash P \to Q$
7. $\{Q\} \vDash P \to Q$
8. $\{P, Q\} \vDash P \leftrightarrow Q$
9. $\{\neg P, \neg Q\} \vDash P \leftrightarrow Q$
10. $\{P, P \to Q\} \vDash Q$

6.1 Example. Determine whether

$$\vDash (P \to (Q \to R)) \to ((P \to Q) \to (P \to R))$$

Solution. We make a truth table for

$$F = (P \to (Q \to R)) \to ((P \to Q) \to (P \to R))$$

P	Q	R	$(P \to (Q \to R))$	$((P \to Q) \to (P \to R))$
1	1	1	1	1
1	1	0	0	0
1	0	1	1	1
1	0	0	1	1
0	1	1	1	1
0	1	0	1	1
0	0	1	1	1
0	0	0	1	1

Here are some relationships between tautologies, equivalences and validity.

$$\begin{aligned} F \equiv G &\Leftrightarrow \vDash (F \leftrightarrow G) \\ &\Leftrightarrow \vDash ((F \to G) \wedge (G \to F)) \\ &\Leftrightarrow \{F\} \vDash G \text{ and } \{G\} \vDash F \end{aligned}$$

When $S = \{F_1, F_2, \ldots, F_n\}$,

$$\begin{aligned} S \vDash G &\Leftrightarrow \{F_1, F_2, \ldots, F_n\} \vDash G \\ &\Leftrightarrow (((F_1 \wedge F_2) \wedge \cdots \wedge F_n) \vDash G \\ &\Leftrightarrow \vDash (((F_1 \wedge F_2) \wedge \cdots \wedge F_n) \rightarrow G \end{aligned}$$

Also

$$\vDash F \Leftrightarrow \emptyset \vDash F$$

$\vDash F$ means for all assignment α, $\alpha(F) = 1$

$\emptyset \vDash F$ means for all assignment α, if (for every $G \in \emptyset, \alpha(G) = 1$) then $\alpha(F) = 1$

Notation. For a set A and a statement or formula F

$$\forall x \in A \;\; F \text{ means } \forall x(x \in A \rightarrow F)$$

and

$$\exists x \in A \;\; F \text{ means } \forall x(x \in A \wedge F)$$

So (for every $G \in \emptyset, \alpha(G) = 1$) is always true. This proves that $\vDash F \Leftrightarrow \emptyset \vDash F$.

6.2 Example. Determine whether

$$(P \vee Q) \rightarrow R \equiv (P \rightarrow R) \wedge (Q \rightarrow R)$$

Solution.

P	Q	R	$(P \vee Q) \rightarrow R$	$(P \rightarrow R) \wedge (Q \rightarrow R)$
1	1	1	1	1
1	1	0	0	0
1	0	1	1	1
1	0	0	0	0
0	1	1	1	1
0	1	0	0	0
0	0	1	1	1
0	0	0	1	1

6.3 Example. Determine whether

$$\{P \rightarrow (Q \vee \neg R), Q \rightarrow \neg P\} \vDash R \rightarrow \neg P$$

Solution.

P	Q	R	$\neg R$	$Q \vee \neg R$	$\neg P$	$P \rightarrow (Q \vee \neg R)$	$Q \rightarrow \neg P$	$R \rightarrow \neg P$
1	1	1	0	1	0	1	0	0
1	1	0	1	1	0	1	0	1
1	0	1	0	0	0	0	1	0
1	0	0	1	1	0	1	1	1
0	1	1	0	1	1	1	1	1
0	1	0	1	1	1	1	1	1
0	0	1	0	0	1	1	1	1
0	0	0	1	1	1	1	1	1

Lecture 7, Sept. 20

7.1 Example. Let F and G be formulas

Determine whether

$$\{F \to G, F \vee G\} \vDash F \wedge G$$

Solution. We make a truth table

F	G	$F \to G$	$F \vee G$	$F \wedge G$
1	1	1	1	1
1	0	0	1	0
0	1	1	1	0
0	0	1	0	0

Remark. It appears from row 3 that the argument is not valid.

But in fact, the argument may or may not be valid, depending on the formulas F and G.

For example, if F is a tautology and G is any formula, the argument is valid.

Or if $F = G$ then the argument is valid.

First-Order Language

Symbol Set

7.2 Definition. A First-Order Language is determined by its symbol set. The symbol set includes symbols from the common symbol set

$$\{\neg, \wedge, \vee, \to, \leftrightarrow, =, \forall, \exists, (,), , \}$$

along with some variable symbols such as

$$x, y, z, u, v, w, \ldots$$

The symbol $=$ is read as "equals". The symbols $\forall$, $\exists$ are called quantifier symbols. The symbol $\forall$ is read as "for all" or "for every", and the symbol $\exists$ is read in "for some" or "there exists".

The symbol set can also include some additional symbols which can include

1. constant symbols
$$a, b, c, \emptyset, 0, i, e, \pi, \ldots$$
2. function symbols
$$f, g, h, \cup, \cap, +, \times, \ldots$$
3. relation symbols
$$P, Q, R, \in, \subset, \subseteq, <, >, =, \ldots$$

The variable and constant symbols are intended to represent elements in a certain set or class u called the universal set or the universal class. The universal set or class is often understood from the context.

Function

7.3 Definition. A unary function f from a set u is a function $f\colon u \to U$ (for every $x \in u$ there is a unique element $y = f(x) \in U$)

A binary function g on u is a function $g\colon u^2 \to U$ where $u^2 = u \times u$ (for every $x, y \in u$ there is a unique element $z = g(x, y) \in U$)

Some binary function symbols are used with infix notation, which means that we write $g(x, y)$ as xgy or as (xgy)

7.4 Example. $+$ is a binary function on $\mathbb{N}$ written with infix notation. So we write $+(x, y)$ as $x + y$ or as $(x + y)$.

Relation

7.5 Definition. A unary relation P on a set u is a subset $P \subseteq U$. For $x \in u$, we write $P(x)$ to indicate that $x \in P$

A binary relation R on u is a subset of U^2. We write $R(x, y)$ to indicate that $(x, y) \in R$

Sometimes a binary relation symbol R is used with indix notation which means that we write $R(x, y)$ as xRy.

7.6 Example. $<$ is a binary relation on $\mathbb{N}$, which means that $<\subseteq \mathbb{N}^2$ and it is used with infix notation, So we write $<(x, y)$ as $x < y$

Also, the symbol $=$ is a binary relation symbol written with infix notation.

Remark. $(P \wedge Q)$ can be written with infix notation as $\wedge PQ$, which is also called polish notation.

Term

7.7 Definition. In a first-order language, a term is a non-empty finite string of symbols from the symbol set which can be obtained by applying the following rules.

1. Every variable symbol is a term and every constant symbol is a term.
2. if f is a unary function symbol and t is a term, then the string $f(t)$ is a term
3. if g is a binary function symbol and s and t are terms, the the string $g(s, t)$ (or the string sgt) is a term.

7.8 Example. The following strings are terms.

- u
- $u \cap v$
- $u \cap (v \cap \emptyset)$
- x
- $x + 1$
- $g(x, f(y + 1))$

Each term represents an element in the universal set or class u

Formula

7.9 Definition. A formula is a non-empty finite string of symbols which can be obtained using the following rules.

1. if P is a unary relation symbol and t is a term then the string $P(t)$ is a formula. (in standard mathematical language we would write $P(t)$ as $t \in P$)
2. if R is a binary relation symbol and s and t are terms then the string $R(s,t)$ is a formula (or sRt)
3. if F is a formula, then so is the string $\neg F$
4. if F and G are formulas then so is each of the strings $F \wedge G$, $F \vee G$, $F \to G$, $F \leftrightarrow G$
5. if F is a formula and x is a variable symbol, then the string $\forall x F$ and $\exists x F$ are both formulas

Examples: Each of the following strings is formula

- $u \subseteq R$
- $\forall u \ \ \emptyset \in u$
- $f(x) < x + 1$
- $x = g(y, z + 1)$

A formula is a formal way of expressing a mathematical statement about element in u, and about functions and relations on u.

Remark. In standard mathematical language, we continually to add new notations which we allow ourselves to use.

7.10 Example. $\dfrac{x+1}{y}$ could be written as $(x + 1)/y$

$\displaystyle\sum_{k=1}^{n} \frac{1}{k}$ could be written as .... (a very long formula)

Lecture 8, Sept. 21

Recap

Symbol Set

Term

Formula

First-Order Language

8.1 Definition. In the language of first-order number theory, we allow us to use the following additional symbols:

$$\{0, 1, +, \times, <\}$$

Unless otherwise stated, we do not allow ourselves to use any other additional symbols.

8.2 Example. Express each of the following statement as formulas in the language of first-order number theory.

a) x is a factor of y

b) x is a prime number

c) x is a power of 3

Solution. We take he universal set to be $\mathbb{Z}$.

a) $\exists z \in \mathbb{Z} \;\; y = x \times z$

b) $1 < x \wedge \forall y(\exists z \;\; x = y \times z \to ((y = 1 \vee y = x) \vee (y + 1 = 0 \vee y + x = 0)))$
$1 < x \wedge \forall y((1 < y \wedge \exists z \;\; x = z \times y) \to y = x)$

c) $(0 < x) \wedge$ the only prime factor of x is 3
$\iff (0 < x) \wedge \forall y \in \mathbb{Z}((\text{y is prime} \wedge \text{y is a factor of x}) \to y = 3)$
$\iff (0 < x) \wedge \forall y \in \mathbb{Z}((1 < y \wedge \exists z \;\; x = y \times z) \to \exists z \;\; y = ((z + z) + z))$

$$x = -y \iff x + y = 0$$
$$x = y - z \iff x + z = y$$

Remark. The two minus signs in the two equations above are different.

8.3 Example. Express the following statements about a function $f \colon \mathbb{R} \to \mathbb{R}$ as formulas in first-order number theory after adding the function symbol f to the symbol set.

a) f is surjective (or onto)

b) f is bijective (or invertible)

c) $\lim_{x \to u} f(x) = v$

Solution. a) $\forall y \in \mathbb{R}\ \exists x \in \mathbb{R}\ y = f(x)$

b) $\forall y \in \mathbb{R}\ \exists! x \in \mathbb{R}\ y = f(x)$
$\iff \forall y \in \mathbb{R}\ (\exists x \in \mathbb{R}(y = f(x) \wedge \forall z(y = f(z) \to z = x)))$

c) $\forall \epsilon > 0\ \exists \delta > 0\ \forall x \in \mathbb{R}(0 < |x - v| < \delta \to |f(x) - v| < \epsilon)$
$\iff \forall \epsilon(0 < \epsilon \to \exists \delta(0 < \delta \wedge \forall x((\neg x = u \wedge (u < x + \delta \wedge x < u + \delta)) \to (v < f(x) + \epsilon \wedge f(x) < v + \epsilon))))$

Lecture 9, Sept. 23

9.1 Definition. In the language of **first-order set theory**, we only use the one additional symbol

$$\in$$

(the membership or "is an element of" symbol), which is a binary relation symbol used with infix notation.

All mathematical statement can be expressed in **this language**

When we use this language, we normally take the universal class to be the class of all sets.

Example: Express each of the following statements about sets as formulas in **first-order set theory**

1. $u = v \backslash (x \cap y)$
2. $u \subseteq P(v \cup w)$
3. $u = 2$

Solution. 1. For sets u, v, x, y

$$\begin{aligned} u = v\backslash(x \cap y) &\iff \forall t(t \in u \leftrightarrow t \in v\backslash(x \cap y)) \\ &\iff \forall t(t \in u \leftrightarrow (t \in v \wedge \neg t \in (x \cap y))) \\ &\iff \forall t(t \in u \leftrightarrow (t \in v \wedge \neg(t \in x \wedge t \in y))) \end{aligned}$$

2.

$$\begin{aligned} u \subseteq P(v \cup w) &\iff \forall x\ (x \in u \to x \in P(v \cup w)) \\ &\iff \forall x\ (x \in u \to \forall y\ (y \in x \to y \in (v \cup w))) \\ &\iff \forall x\ (x \in u \to \forall y\ (y \in x \to (y \in v \vee y \in w))) \end{aligned}$$

3.

$$\begin{aligned} u = 2 &\iff u = \{\emptyset, \{\emptyset\}\} \\ &\iff \forall x\ (x \in u \leftrightarrow x \in \{\emptyset, \{\emptyset\}\}) \\ &\iff \forall x\ (x \in u \leftrightarrow (x = \emptyset \vee x = \{\emptyset\})) \\ &\iff \forall x\ (x \in u \leftrightarrow (\forall y\ \neg y \in x \vee \forall y\ y \in x \leftrightarrow y = \emptyset)) \\ &\iff \forall x\ (x \in u \leftrightarrow (\forall y\ \neg y \in x \vee \forall y\ y \in x \leftrightarrow (\forall z\ \neg z \in y))) \end{aligned}$$

The ZFC axioms can all be expressed as formulas in first order set theory.

1. Equality Axiom:
$$\forall u \forall v\ (u = v \leftrightarrow \forall x\ (x \in u \leftrightarrow x \in u))$$
2. Empty Set Axiom:
$$\exists u \forall x\ \neg x \in u$$

3. Pair Axiom:
$$\forall u \, \forall v \, \exists w \, \forall x \; (x \in w \leftrightarrow (x = u \vee x = v))$$

4. Union Axiom:
$$\forall u \, \exists w \, \forall x \; (x \in w \leftrightarrow \exists v \; (v \in u \cup x \in v))$$

Proof. When we do mathematical proofs, one of the things we allow ourselves to do is make use of some equivalences.

When F, G, H are formulas, s, t are terms, and x, y are variables, the following are equivalences which we call **basic equivalence**

1. $F \equiv F$
2. $\neg\neg F \equiv F$
3. $F \wedge F \equiv F$
4. $F \vee F \equiv F$
5. $F \wedge G \equiv G \wedge G$
6. $F \vee G \equiv G \vee F$
7. $(F \wedge G) \vee H \equiv F \wedge (G \vee H)$
8. $(F \vee G) \wedge H \equiv F \vee (G \wedge H)$
9. $F \wedge (G \vee H) \equiv (F \wedge G) \vee (F \wedge H)$
10. $F \vee (G \wedge H) \equiv (F \vee G) \wedge (F \vee H)$
11. $\neg(F \wedge G) \equiv \neg F \vee \neg G$
12. $\neg(F \vee G) \equiv \neg F \wedge \neg G$
13. $F \to G \equiv \neg G \to \neg F$
14. $F \to G \equiv \neg F \vee G$
15. $\neg(F \to G) \equiv F \wedge \neg G$
16. $F \leftrightarrow G \equiv (F \to G) \wedge (G \to F)$
17. $F \leftrightarrow G \equiv (\neg F \vee G) \wedge (\neg G \vee F)$
18. $F \leftrightarrow G \equiv (F \wedge G) \vee (\neg F \wedge G)$
19. $F \wedge (G \vee \neq G) \equiv F$
20. $F \vee (G \vee \neq G) \equiv (G \vee \neq G)$
21. $F \wedge (G \wedge \neg G) \equiv G \wedge \neg G$
22. $F \vee (G \wedge \neg G) \equiv F$

□

Note. We can use basic equivalences one at a time, to derive other equivalences.

9.2 Example. Derive the equivalence:

$$(F \vee G) \to H \equiv (F \to H) \wedge (G \to H)$$

Solution.

$$\begin{aligned}
(F \vee G) \to H &\equiv \neg(F \vee G) \vee H \text{ (by the equivalence)} \\
&\equiv (\neg F \wedge \neg G) \vee H \text{ (by the de Morgan's)} \\
&\equiv H \vee (\neg F \wedge \neg G) \text{ (by the Commutativity)} \\
&\equiv (H \vee \neg F) \wedge (H \vee \neg G) \text{ (by the Distributivity)} \\
&\equiv (\neg F \vee H) \wedge (\neg G \vee H) \text{ (by the Commutativity)} \\
&\equiv (F \to H) \wedge (G \to H) \text{ (by the equivalence)}
\end{aligned}$$

9.3 Definition. Here are some more basic equivalences.

1. $s = t \equiv t = s$
2. $\forall x \, \forall y \; F \equiv \forall y \, \forall x \; F$
3. $\exists x \, \exists y \; F \equiv \exists y \, \exists x \; F$
4. $\neg \forall x \; F \equiv \exists x \; \neg F$
5. $\neg \exists x \; F \equiv \forall x \; \neg F$
6. $\forall x \; (F \wedge G) \equiv \forall x \; F \wedge \forall x \; G$
7. $\exists x \; (F \vee G) \equiv \exists x \; F \vee \exists x \; G$

Lecture 10, Sept. 26

10.1 Example.

$$\begin{aligned}\exists x\ (F \to G) &\equiv \exists X\ (\neg F \vee G)\\ &\equiv \exists x\ \neg F \vee \exists x\ G\\ &\equiv \neg\forall x\ F \vee \exists x\ G\\ &\equiv \forall x\ F \to \exists x\ G\end{aligned}$$

10.2 Definition. In a formula f, every occurrence of a variable symbol x (Except when the occurrence of x immediately follows a quantifier $\forall, \exists$) is either **free** or **bound**.

In the formulas $\forall x\ F$ and $\exists x\ F$, every free occurrence of x in F becomes **bound** by the initial quantifier, and every bound occurrence of x in F remains bound (by the same quantifier which binds it in F).

10.3 Example.

$$\forall y\ (x \times y = y \times x)$$

Both occurrence of x are free, and both occurrence of y are bound by the initial quantifier.

$$\forall x\ (\forall y\ (x \times y = y \times x) \to x \times a = a \times x)$$

10.4 Definition. An **interpretation** in a first-order language consists of the following: a choice of the universal set u, and a choice of meaning for each constant, function and relation symbol.

A formula is a meaningless string of symbols until we choose an interpretation. Once we choose an interpretation, a formula becomes a meaningful mathematical statement about its free variables.

The truth or falsehood of a formula may still depend on the value in u which are assigned to the free variable symbols in F.

An assignment (of values in u to the variable symbols) is a function $\alpha : \{\text{variable symbols}\} \to u$

10.5 Example. Consider the formula

$$\forall y\ (x \times y = y \times x)$$

when $u = \mathbb{R}$ (and $\times$ is multiplication) the formula becomes true (for any value assigned to x).

when $u = \mathbb{R}^3$ annd $\times$ is cross-product, the formula is true iff $x = 0$

when u is the set of all $n \times n$ matrices with entries in $\mathbb{R}$, and $\times$ denotes matrix multiplication, the formula is can be read as "the matrix x commutes with every matrix", and it is true iff $x = cI$ for some $c \in \mathbb{R}$

Notation. For a formula F, a variable symbol x and a term t, we write $[F]_{x \mapsto t}$ to denote the formula which is constructed from F by replacing x by t.

In an interpretation, the formula $[F]_{x \mapsto t}$ has the same meaning about t that f has about x.

Roughly speaking, $[F]_{x \mapsto t}$ is obtained from F by replacing each free occurrence of the symbol x by the term t. (but if a variable symbol in t would become bound by this replacement, we rename the variable first.)

10.6 Example. In $u = \mathbb{Z}$, $x \mid y$ means $\exists z\ y = x \times z$

$|\exists z\ y = x \times z|_{y \mapsto u} = \exists z\ u = x \times z$ means $x \mid u$

$|\exists z\ y = x \times z|_{y \mapsto x} = \exists z\ x = x \times z$ means $x \mid x$

$|\exists z\ y = x \times z|_{y \mapsto z} \neq \exists z\ z = x \times z$

$|\exists z\ y = x \times z|_{y \mapsto z} = |\exists u\ y = x \times u|_{y \mapsto z} = \exists u\ z = x \times u$

Here are some more basic equivalences:

E32 $\forall x\ F \equiv F$ if x is not free in F

E34 $\forall x\ F \equiv \forall y\ [F]_{x \mapsto y}$ if y is not free in F

Lecture 11, Sept. 27

11.1 Definition. Interpretation is a choice of a non-empty set u, and constant, functions and relations for each constant, function and relation symbol.

An **Assignment** in u,

$$\alpha\colon \{\text{variale symbols}\} \to u$$

We write $\alpha(F) = 1$ when F is true in u under α.

We write $\alpha(F) = 0$ when F is false in u under α.

We say F is true in u when $\alpha(F) = 1$ for **every** assignment $\alpha \in u$

11.2 Example. the formula $x \times y = y \times x$ is true in $\mathbb{Z}$ but not true in $n \times n$ matrices.

11.3 Definition. For formulas F and G and a set of formulas S, we say that F is a **tautology** and we write $\vDash F$, when for every interpretation u and every assignment $\alpha \in u$, $\alpha(F) = 1$

11.4 Definition. We say that F and G are **equivalent**, and we write $F \equiv G$, when for every interpretation u, for every assignment $\alpha \in u$, $\alpha(F) = \alpha(G)$, we say that the argument "F there fore G" is valid, or that "S induces G", or that "G is a consequences of S", when for every interpretation u and for every assignment $\alpha \in u$, if $\alpha(F) = 1$ for every $F \in S$ then $\alpha(G) = 1$

11.5 Definition. Given a formula G and a set of formulas S, such that $S \vDash G$, a **derivation** for the valid argument $S \vDash G$ is a list of valid arguments

$$S_1 \vDash G_1, S_2 \vDash G_2, S_3 \vDash G_3, \ldots$$

where for some index k we have $S_k = S$ and $G_k = G$, such that each valid argument in the list is obtained from previous valid arguments in the list by applying one of the basic validity rules.

1 Basic Validity Rules

Each basic validity rule is a formal and precise way of describing standard method of mathematical proof.

Rules V1, V2 and V3 are used in derivations because we make a careful distinction between **premises** and **conclusions**. In standard mathematical proofs we do not make a careful distinction.

Premise V1. If $F \in S$ then $S \vDash F$. In words, if we assume F, we can conclude F.

V2. If $S \vDash F$ and $S \subseteq \mathcal{T}$ then $\mathcal{T} \vDash F$. In words, if we can prove F without assuming G, then we can still prove F if we assume G.

Chain Rule V3. If $S \vDash F$ and $S \cup \{F\} \vDash G$ then $S \vDash G$. In words, if we can prove F, and by assuming F we can prove G, then we can prove G directly without assuming F.

Proof by Cases V4. If $S \cup \{F\} \vDash G$ and $S \cup \{\neg F\} \vDash G$ then $S \vDash G$. In words, in either case G is true.

Contradiction V5. If $S \cup \{\neg F\} \vDash G$ and $S \cup \{\neg F\} \vDash \neg G$ then $S \vDash F$. In words, to prove F by contradiction, we suppose, for a contradiction, that F is false, we choose a formula G, then we prove that G is true and we prove that G is false.

V6. If $S \cup \{F\} \models G$ and $S \cup \{F\} \models \neg G$ then $S \models \neg F$

V7. If $S \models F$ and $S \models \neg F$ then $S \models G$

Conjunction V8. $S \models F \wedge G \iff (S \models F$ and $S \models G)$

V9. If $S \cup \{F, G\} \models H$ then $S \cup \{F \wedge G\} \models H$

V10. ...

V11. ...

V12. ...

Disjunction V13. $S \models F \vee G \iff S \cup \{\neg F\} \models \iff S \cup \{\neg G\} \models F$

V14. ...

Lecture 12, Sept. 28

V13. How to prove an or statement

V14. $S \cup F \vDash H$ and $S \cup G \vDash H \iff S \cup (F \vee G) \vDash H$

V15. In words, from F we can conclude $F \vee G$

V16.

V17. In words, from $F \vee G$ and $\neg F$ we can conclude G

V18.

...

V25. In words, to prove $F \iff G$ we suppose F then prove G, and we suppose G and prove F

V26. $(F \iff G) \equiv (F \wedge G) \vee (\neg F \wedge \neg G)$

...

V33. $S \vDash t = t$. In words, we can always conclude that $t = t$ is true under any assumptions.

V34. From $s = t$ we can conclude $t = s$

V35. From $r = s$ and $s = t$ we can conclude $r = t$

V36. If $S \vDash s = t$ then $(S \vDash [F]_{x \mapsto t} \iff S \vDash [F]_{x \mapsto s})$. In words, if $\vDash s = t$, we can always replace any occurrence of the term s by the term t.

V37. If $S \vDash [F]_{x \mapsto y}$ and y is not free in $S \cup \{\forall x\ F\}$ then $S \vDash \forall x\ F$

If have not made any assumptions about x (earlier in out proof) then to prove $\forall x\ F$ we write "let x be arbitrary" then we prove F.

If we have not made any assumptions about y, then to prove $\forall x\ F$, we write "let y be arbitrary" then prove $[F]_{x \mapsto y}$

(This is related to the equivalence

$$\forall x\ F \equiv \forall y\ [F]_{x \mapsto y}$$

)

V38. If $S \vDash \forall x\ F$, then $S \vDash [F]_{x \mapsto t}$

V39.

V40. If $S \cup \{[F]_{x \mapsto t}\} \vDash G$ then $S \vDash \exists X\ F$. In words, to prove $\exists x\ F$ we choose any term t, and prove $[F]_{x \mapsto t}$.

V41. If y is not free in $S \cup \{\exists x\ F, G\}$ and if $S \cup [F]_{x \mapsto y} \vDash G$ then $S \cup \exists x\ F \vDash G$. In words, to prove that $\exists x\ F$ implies G, choose a variable y which we have not made assumptions about and which does not occur in G, we write "choose y so that $[F]_{x \mapsto y}$ is true", then prove G.

Note. In standard mathematical language,

$$\forall x \ \in A \ F$$

means

$$\forall x \ (x \in a \to F)$$

To prove $\forall x \ (x \in a \to F)$ we write "let x be arbitrary", then prove $x \in a \to F$ which we do by writing "suppose $x \in A$" then prove F.

Usually, instead of writing "let x be arbitrary" and "suppose $x \in A$ " we write "let $x \in A$ be arbitrary" or simply "let $x \in A$".

So to prove $\forall x \in A \ F$ we write "let $x \in A$" then prove F. Alternatively, write "let $y \in A$" then prove $[F]_{x \mapsto y}$.

12.1 Example. Prove that

$$\{F \to (G \wedge H), (F \wedge G) \vee H\} \vDash H$$

For all assignment $\alpha \colon \{P, Q, R, \dots\} \to \{0, 1\}$, if $\alpha(F \to (G \wedge H)) = 1$ and $\alpha((F \wedge G) \vee H) = 1$ then $\alpha(H) = 1$

Proof. Let α be an arbitrary assignment. Suppose that $F \to (G \wedge H)$ is true (under α), and $(F \wedge G) \vee H$ is true (under α).

Suppose, for a contradiction, that H is false.

$$\begin{array}{ll} (F \wedge G) \vee H, \neg H & \therefore F \wedge G \\ (F \wedge G) & \therefore F \\ F \to (G \wedge H), F & \therefore G \wedge H \\ G \wedge H & \therefore H \\ \neg H, H & \textit{gives the contradiction} \\ \therefore H & \end{array}$$

□

Lecture 13, Sept. 30

13.1 Example.

$$\{F \to (G \wedge H), (F \wedge G) \vee H\} \vDash H$$

Proof. Proof by contradiction. Suppose H is false

$$\begin{array}{ll} (F \wedge G) \vee H, \neg H & \therefore F \wedge G \\ (F \wedge G) & \therefore F \\ F \to (G \wedge H), F & \therefore G \wedge H \\ G \wedge H & \therefore H \\ \neg H, H & \textit{gives the contradiction} \\ \therefore H & \end{array}$$

□

Here is a derivation for the valid argument

$S = \{F \to (G \wedge H), (F \wedge G) \vee H, \neg H\} \vDash F \to (G \wedge H)$	*by V1*
$S \vDash (F \wedge G) \vee H$	*by V1*
$S \vDash \neg H$	*V1*
$S \vDash F \wedge G$	*V18 on line 2,3*
$S \vDash F$	*V11 on line 4*
$S \vDash G \wedge H$	*V23 on line 1,5*
$S \vDash H$	*by V12 on 6*
$\{F \to (G \wedge H), (F \wedge G) \vee H\} \vDash H$	*V5 on line 3,7*

Here is another proof

Proof. Let α be an arbitrary assignment

Suppose that $F \to (G \wedge H)$ is true (under α)

Suppose that $(F \wedge G) \vee H$ is true

Note that wither $F \wedge G$ is true or H is true

Case 1. Suppose $F \wedge G$ is true. [V14]

Since $F \wedge G \therefore F$ [V11]

Since $F \to (G \wedge H)$ and $F \therefore F$ [V23]

Since $G \wedge H \therefore H$ [V12]

Case 2. Support that H is true. [V14]

Then H is true. [V1]

In either case, we have proven H [V14]

□

Here is a corresponding derivation of valid argument

1. $S = \{F \to (G \wedge H), (F \wedge G)\} \vDash F \to (G \wedge H)$
2. $S \vDash F \wedge G$
3. $S \vDash F$
4. $S \vDash G \wedge H$
5. $S \vDash H$
6. $\{F \to (G \wedge H), H\} \vDash H$
7. $\{F \to (G \wedge H), (F \wedge G) \vee H\} \vDash H$

13.2 Example. Show that

$$\{(F \vee \neg G) \to H, F \leftrightarrow (G \wedge \neg H)\} \vDash \neg(H \to F)$$

Solution: We need to show that

for every assignment α

if $(F \vee \neg G) \to H$ is true under α

and $F \leftrightarrow (G \wedge \neg H)$ is true

then $H \to F$ is false

Proof. Let α be arbitrary assignment

Suppose $(F \vee \neg G) \to H$ is true

Suppose $F \leftrightarrow (G \wedge \neg H)$ is true.

[We need to show that $H \to F$ is false. Notice that $\neg(H \to F) \equiv H \wedge \neg F$. So we need to show that H is true and F is false.]

Suppose, for a contradiction, that H is false.

Since $(F \vee \neg G) \to H$ and $\neg H \quad \therefore \neg(F \vee \neg G)$

Since $\neg(F \vee \neg G) \quad \therefore \neg F \wedge G$

Since $F \leftrightarrow (G \wedge \neg H)$ and $\neg F \quad \therefore \neg(G \wedge \neg H)$

Since G and $\neg H \quad \therefore G \wedge \neg H$

Since $G \wedge \neg H$ and $\neg(G \wedge \neg H)$ we have a contradiction

So H is true.

Since H is true, then $\neg\neg H$

Since $\neg\neg H$ we have $\neg G \vee \neg\neg H$

Since $\neg G \vee \neg\neg H$ we have $\neg(G \wedge \neg H)$

Since $F \leftrightarrow (G \wedge \neg H)$ and $\neg(G \wedge \neg H)$, we have $\neg F$

Since H and $\neg F$, we have $H \wedge \neg F$

Since $H \wedge \neg F$ we have $\neg(H \rightarrow F)$

□

$$\{(F \vee \neg G) \rightarrow H, F \leftrightarrow (G \wedge \neg H)\} \vDash \neg(H \rightarrow F)$$

Here is a derivation

Proof.

1.	$S = \{(F \vee \neg G) \rightarrow H, F \leftrightarrow (G \wedge \neg H), \neg H\} \vDash \neg(H \rightarrow F)$	v1
2.	$S \vDash F \leftrightarrow (G \wedge \neg H)$	v1
3.	$S \vDash \neg H$	v1
4.	$S \vDash \neg(F \vee \neg G)$	v24
5.	$S \vDash \neg F \wedge \neg\neg G$	v45,E8
6.	$S \vDash \neg F \wedge G$	v11 on 5
7.	$S \vDash \neg F$	v31 on 2,6
8.	$S \vDash \neg\neg G$	12 on 5
9.	$S \vDash G$	v45,e2 on 8
10.	$S \vDash G \wedge \neg H$	v10 on 9,3
11.	$T = \{(F \wedge \neg G) \rightarrow H, F \leftrightarrow (F \wedge \neg H)\} \vDash H$	v5 on 10,7
12.	$T \vDash \neg\neg H$	
13.	$T \vDash \neg G \vee \neg\neg H$	
14.	$T \vDash \neg(G \wedge \neg H)$	
15.	$T \vDash F \leftrightarrow (G \wedge \neg H)$	
16.	$T \vDash \neg F$	
17.	$T \vDash H \wedge \neg F$	
18.	$T \vDash \neg(H \rightarrow F)$	

□

Lecture 14, Oct. 3

14.1 Example.

$$\vDash \forall x\ (\exists y\ \neg xRy \vee \exists y\ yRx)$$

Solution.

$$\begin{aligned} & \forall x\ (\exists y\ \neg xRy \vee \exists y\ yRx) \\ [E28] \equiv & \forall x\ (\neg \forall y\ xRy \vee \exists y\ yRx) \\ [E20] \equiv & \forall x\ (\forall y\ xRy \to \exists y\ yRx) \end{aligned}$$

Proof. Let u be an arbitrary non-empty set. Let R be an arbitrary binary relation on u (that is $R \subseteq u^2$)

Let $x \in u$ be arbitrary.

Suppose that $\forall y\ xRy$.

Then in particular we have xRx. [V38]

Since xRx it follows that $\exists y\ yRx$. [V40]

We have proven that $\forall y\ xRy \to \exists y\ yRx$. [V19]

Since x was arbitrary, we have proven that $\forall x\ (\forall y\ xRy \to \exists y\ yRx)$. [V37]

Since u and R are arbitrary, we have proven that $\vDash \forall x\ (\forall y\ xRy \to \exists y\ yRx)$. [V37, V19]

Since equivalence, we have proven that $\vDash \forall x\ (\exists y\ \neg xRy \vee \exists y\ yRx)$.

□

Here is a derivation

1	$\{\forall y\ xRy\} \vDash \forall y\ xRy$	V1
2	$\{\forall y\ xRy\} \vDash xRx$	V38 on 1
3	$\{\forall y\ xRy\} \vDash \exists y\ yRx$	V40 on 2
4	$\vDash (\exists y\ xRy \to \exists y\ yRx)$	V19 on 3
5	$\vDash (\neg \forall y\ xRy \vee \exists y\ yRx)$	V45, E20
6	$\vDash (\exists y\ \neg xRy \vee \exists y\ yRx)$	V45, E28
7	$\forall x\ (\exists y\ \neg xRy \vee \exists y\ yRx)$	V37 on 6

14.2 Example. For $a, b, c \in \mathbb{Z}$, show that if $a \mid b$ and $b \mid c$ then $a \mid c$

(We say a divides b, or a is a factor of b, of b is a multiple of a, and we write $a \mid b$, when $\exists x\ b = a \cdot x$)

Here is a proof in standard mathematical language.

Proof. Let $a, b, c \in \mathbb{Z}$ be arbitrary.

Suppose that $a \mid b$ and $b \mid c$.

Since $a \mid b$, choose $u \in \mathbb{Z}$ so that $b = a \cdot u$

Since $a \mid b$, choose $v \in \mathbb{Z}$ so that $c = b \cdot v$

Since $b = a \cdot u$ and $c = b \cdot v$

We have $c = (a \cdot u) \cdot v = a \cdot (u \cdot v)$

Thus $a \mid c$ (we have $\exists x\ c = a \cdot x$ choose $x = u \cdot v$)

□

Here is a step-by-step proof to show that

$$\{\exists x\ b = a \times x, \exists x\ c = b \times x, \forall x\, \forall y\, \forall z\ ((x \times y) \times z) = (x \times (y \times z))\} \vDash \exists x\ c = a \times x$$

V37, v19. Let U be a non-empty set,

[V37, v19] Let $\times$ be a binary function on U.

[V9] Suppose $\exists x\ b = a \times x$,

[V9] Suppose $\exists x\ c = b \times x$,

[V9] Suppose $\forall x\, \forall y\, \forall z\ ((x \times y) \times z) = (x \times (y \times z))$

[V41] Since $\exists x\ b = a \times x$, we can choose $u \in U$ so that $b = a \times u$

[V41] Since $\exists x\ c = b \times x$, we can choose $v \in U$ so that $c = b \times v$

[V36]Since $b = a \times u$ and $c = b \times v$, we have $c = (a \times u) \times v$

[V38] Since $\forall x\, \forall y\, \forall z\ ((x \times y) \times z) = (x \times (y \times z))$ we have $\forall y\, \forall z\ ((a \times y) \times z) = (a \times (y \times z))$

[V38] Since $\forall y\, \forall z\ ((a \times y) \times z) = (a \times (y \times z))$ we have $\forall z\ ((a \times u) \times z) = (a \times (u \times z))$

[V38] Since $\forall z\ ((a \times u) \times z) = (a \times (u \times z))$ we have $((a \times u) \times v) = (a \times (u \times v))$.

[V35] Since $c = (a \times u) \times v$ and $((a \times u) \times v) = (a \times (u \times v))$, we have $c = a \times (u \times v)$

[V40] Since $c = a \times (u \times v)$ we have proven that $\exists x\ c = a \times x$

□

Lecture 15, Oct. 4

15.1 Definition. An **ordered n-tuple** with entries in a set A, is a function $a\colon \{1,2,3,\dots\} \to A$ where we write $a(k)$ as a_k.

We write $a = (a_1, a_2, \dots)$ to indicate that $a = \{1,2,3,\dots\} \to A$ is given by $a(k) = a_k$ for $k \in \{1,2,3,\dots,n\}$

The set of all such n-tuples is denoted by A^n

$$A^n = \{(a_1, a_2, \dots) \mid \ each\ a_{\mathbb{Z}} \in A\}$$

15.2 Definition. A **sequence** with **entries** or **terms** in a set A is a function

$$a\colon \{1,2,3,\dots\} \to A$$

Where we write $a(k) = a_k$ or sometimes a function

$$a\colon \{m, m+1, m+2, \dots\} \to A$$

where $m \in \mathbb{Z}$.

We write $a = (a_k)_{k \geq m} = (a_m, a_{m+1}, \dots)$

or we write $a = \{a_k\}_{k \geq m} = \{a_m, a_{m+1}, \dots\}$

to indicate that $a = \{m, m+1, \dots\} \to A$ is given by $a(k) = a_k$

Remark. For sets A and B we define A^B to be the set of all functions

$$f\colon B \to A$$

Also the integer n is defined to be

$$n = \{0, 1, 2, \dots, n-1\}$$

So Actually

$$A^n = A^{\{0,1,2,\dots,n-1\}} = \{a\colon \{0,1,\dots,n-1\} \to A\}$$

and we write elements in A^n as $(a_0, a_1, \dots a_{n-1})$

And the set of sequences with entries in A is the set $A^{\mathbb{N}} = \{a\colon \{0,1,2,\dots\} \to A\}$

15.3 Definition. We say that a sequence is defined in **closed-form** when we are given a formula for a_k in terms of k.

We say that a sequence is defined **recursively** when we are given a formula for a_n in terms of k and in terms of previous terms a_i in the sequence.

15.4 Example. Fibonacci Sequence

$$a_{n+2} = a_{n+1} + a_n$$

15.5 Example. When we write

$$S_n = \sum_{k=1}^{n} \frac{1}{k^2} = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \dots$$

we mean that $S_1 = 1$ and $S_n = S_{n-1} + \dfrac{1}{n^2}$

15.6 Example. When we write

$$P_n = \prod_{k=1}^{n} \frac{2k-1}{2k}$$

We mean that $P_1 = \dfrac{1}{2}$ and $P_n = P_{n-1} \cdot \dfrac{2n-1}{2n}$

15.7 Example. When we write $n!$, we mean that $0! = 1$ and $n! = (n-1)! \cdot n$ for $n \geq 1$

15.8 Example. In Set Theory, we define addition on $\mathbb{N}$, recursively as follows

$$0 = \emptyset, 1 = \{0\}, x + 1 = x \cup \{x\}$$

For $n \in \mathbb{N}$, $n + 0 = n$, $n + (m + 1) = (n + m) + 1 = (n + m) \cup \{(n + m)\}$

15.9 Theorem. ***Mathematical Induction*** *Let $F(n)$ be a mathematical statement about an integer n. Let $m \in \mathbb{Z}$*

Suppose $F(m)$ is true. (that is $[F]_{n \mapsto m}$)

Suppose that for all $k \geq m$, if $F(k)$ is true then $F(k+1)$ is true.

Then $F(n)$ is true for all $n \geq m$.

15.10 Example. Define a_n recursively by $a_1 = 1$ and $a_{n+1} = \dfrac{n}{n+1} \cdot a_n + 1$. Find a closed-form formula for a_n

Solution. We have $a_1 = 1$, $a_2 = \dfrac{3}{2}$, $a_3 = \dfrac{4}{2}, \ldots$

It appears that $a_n = \dfrac{n+1}{2}$

When $n = 1, \cdots$

Suppose $a_k = \dfrac{k+1}{2}$

When $n = k + 1$ we have

$$\begin{aligned} a_n = a_{k+1} &= \frac{k}{k+1} \cdot a_k + 1 \\ &= \frac{k}{k+1} \cdot \frac{k+1}{2} + 1 \\ &= \frac{k+2}{2} \\ &= \frac{(k+1)+1}{2} \\ &= \frac{n+1}{2} \end{aligned}$$

By induction, $a_n = \dfrac{n+1}{2}$ forall $n \geq 1$

15.11 Exercise.

1. $$\sum_{k=1}^{n} k^3$$

2. $$\prod_{k=1}^{n} (1 - \frac{1}{k^2})$$

Lecture 16, Oct. 5

16.1 Theorem. *Let $F(n)$ be a statement about an integer n. Let $m \in \mathbb{Z}$*

Suppose $F(m)$ is true

Suppose that for all $k \geq m$, if $F(k)$ is true then $F(k+1)$ is true

Then $F(n)$ is true for all $n \geq m$

Proof Method Let $F(n)$ be a statement about an integer and let $m \in \mathbb{Z}$

To prove $F(n)$ is true for all $n \geq m$, we can do the following.

1. Prove that $F(n)$ is true
2. Let $k \geq m$ be arbitrary and suppose, inductively, that $F(k)$ is true
3. Prove $F(k+1)$ is true

Alternatively, suppose $F(k-1)$ prove $F(k)$

A slightly different proof method To prove that $F(n)$ is true for all $n \geq m$ we can do the following:

1. Prove that $F(m)$ is true and that $F(m+1)$ is true
2. Let $k \geq m+2$ be arbitrary and suppose that $F(k-1)$ and $F(k-2)$ are true
3. Prove that $F(k)$ is true

Another Proof Method we can prove that $F(n)$ is true for all $n \geq m$ as follows.

1. Let $n \geq m$ be arbitrary and suppose that $F(k)$ is true for all k with $m \leq k < n$
2. prove that $F(n)$ is true.

16.2 Theorem. ***Strong Mathematical Induction*** *Let $F(n)$ be a statement about an integer n and let $m \in \mathbb{Z}$*

Suppose that for all $n \geq m$, if $F(k)$ for all $k \in \mathbb{Z}$ with $m \leq k < n$, then $F(n)$ is true.

Then $F(n)$ is true for all $n \geq m$.

Proof. Let $G(n)$ be a statement "F(n) is true for all $k \in \mathbb{Z}$ with $m \leq k < n$"

Note that $G(m)$ is true vacuously. (since there is no value of $k \in \mathbb{Z}$ with $m \leq k < n$)

Let $n \geq m$ be arbitrary.

Suppose $G(n)$ is true, that is "$F(n)$ is true for all $k \in \mathbb{Z}$ with $m \leq k < n$"

Since $F(n)$ is true for all $k \in \mathbb{Z}$ with $m \leq k < n$, then $F(n)$ is true for all $k \in \mathbb{Z}$ with $m \leq k < n+1$. In other words, $G(n+1)$ is true.

Now let $n \geq m$ be arbitrary. Since $G(k)$ is true for all $k \geq m$, in particular $G(n+1)$. In other words, $F(k)$ is true for all k with $m \leq k < n+1$. In particular $F(n)$ is true

Since $n \geq m$ was arbitraty, $F(n)$ is true for all $n \geq m$. □

16.3 Example. Let $(x_n)_{n\geq 0}$ be the sequence which is defined recursively by $x_0 = 2$, $x_1 = 2$ and $x_n = 2x_{n-1} + 3x_{n-2}$ for all $x \geq 2$

Find a closed formula for x_n

Solution. Observe that $x_n = 3^n + (-1)^n$

When $n = 0$, $x_0 = 2$ and $3^0 + (-1)^0 = 2$, so $x_n = 3^n + (-1)^n$ is true when $n = 0$

When $n = 1$, $x_1 = 2$ and $3^1 + (-1)^1 = 2$, so $x_n = 3^n + (-1)^n$ is true when $n = 1$

Let $n \geq 2$ be arbitrary.

Suppose that $x_{n-1} = 3^{n-1} + (-1)^{n-1}$ and $x_{n-2} = 3^{n-2} + (-1)^{n-2}$

$$\begin{aligned} x_n &= 2x_{n-1} + 3x_{n-2} \\ &= 2(3^{n-1} + (-1)^{n-1}) + 3(3^{n-2} + (-1)^{n-2}) \\ &= 9^{n-2} + (3-2)(-1)^{n-2} \\ &= 3^n + (-1)^n \end{aligned}$$

By induction, $x_n = 3^n + (-1)^n$ for all $n \geq 0$

Binomial Theorem

16.4 Definition. For $n, k \in \mathbb{N}$ with $0 \leq k \leq n$

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)(n-2)\dots(n-k+1)}{k!}$$

Lecture 17, Oct. 7

Binomial Theorem

17.1 Definition. For $n, k \in \mathbb{N}$ with $0 \leq k \leq n$

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)(n-2)\dots(n-k+1)}{k!}$$

The number of ways to choose k of n objects,

1. If we choose the k objects with replacement (or with repetition), and if order matters, is n^k
2. If we choose the k objects without replacement, and if order matters, is $\frac{n!}{(n-k)!}$. (In particular the number of ways to arrange n objects is $n!$)
3. If we choose the k objects without replacement, and if order does not matters (so we form a k-element set), is $\binom{n}{k} = \frac{n!}{k!(n-k)!}$

Note. For $n, k \in \mathbb{N}$ with $0 \leq k \leq n$, $\binom{n}{0} = 1$, $\binom{n}{n} = 1$, $\binom{n}{k} = \binom{n}{n-k}$, $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$

Proof.

$$\begin{aligned}
\binom{n}{k} + \binom{n}{k+1} &= \frac{n!}{k!(n-k)!} + \frac{n!}{(k+1)!(n-k-1)!} \\
&= \frac{n!(k+1)}{(k+1)!(n-k)!} + \frac{n!(n-k)!}{(k+1)!(n-k)!} \\
&= \frac{n!(k+1+n-k)}{(k+1)!(n-k)!} \\
&= \frac{(n+1)!}{(k+1)!(n+1-k-1)!} \\
&= \binom{n+1}{k+1}
\end{aligned}$$

□

Pascal Triangle

17.2 Example.

$$(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5$$

17.3 Theorem. ***Binomial Theorem*** *For $a, b \in \mathbb{R}$ and $n \in \mathbb{N}$ we have the following formula*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

Proof. When $n = 0$,

$$(a+b)^0 = 1$$
$$\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} = \binom{0}{0} a^0 b^0 = 1$$

When $n = 1$,

$$(a+b)^1 = a + b$$
$$\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} = \binom{1}{0} a^1 b^0 + \binom{1}{1} a^0 b^1 = a + b$$

Let $n \geq 1$ be arbitrary.

Suppose, inductively, that

$$(a+b)^n = \binom{n}{0} a^n + \binom{n}{1} a^{n-1} b + \binom{n}{2} a^{n-2} b^2 + \cdots + \binom{n}{n-1} a^1 b^{n-1} + \binom{n}{n} b^n$$

Then

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)(a+b)^n \\
&= (a+b)(\binom{n}{0} a^n + \binom{n}{1} a^{n-1} b + \cdots + \binom{n}{n-1} a^1 b^{n-1} + \binom{n}{n} b^n) \\
&= \binom{n}{0} a^{n+1} + \binom{n}{1} a^n b + \cdots + \binom{n}{n-1} a^2 b^{n-1} + \binom{n}{n} a b^n \\
&\qquad + \binom{n}{0} a^n b + \binom{n}{1} a^{n-1} b^2 + \cdots + \binom{n}{n-1} a^1 b^n + \binom{n}{n} b^{n+1} \\
&= \binom{n+1}{0} a^{n+1} + \binom{n+1}{1} a^n b + \cdots + \binom{n+1}{n} a b^n + \binom{n+1}{n+1} b^{n+1} \\
&= \sum_{k=0}^{n+1} \binom{n}{k} a^k b^{n-k}
\end{aligned}$$

By induction, it follows that $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$ for all $n \geq 0$ □

17.4 Example.

$$(x+2)^6 = x^6 + 12x^5 + 60x^4 + 160x^3 + 240x^2 + 192x + 64$$

17.5 Example. Find the coefficient of x^8 in the expansion of

$$(5x^3 - \frac{2}{x^2})^{11}$$

Solution.

$$\begin{aligned}
(5x^3 - \frac{2}{x^2})^{11} &= \sum_{k=0}^{11} \binom{11}{k} (5x^3)^{11-k} (-\frac{2}{x^2})^{11} \\
&= \sum_{k=0}^{11} (-1)^k \binom{11}{k} 5^{11-k} 2^k x^{3(11-k)-2k}
\end{aligned}$$

To get $3(11-k)-2k=8$ that is $k=5$

So that the coefficient of x^8 is $(-1)^5\binom{11}{5}5^{11-5}2^5=-231000000$

17.6 Example. Find

$$\sum_{k=0}^{n}\binom{2n}{2k}\frac{1}{2^k}$$

Solution.

$$(1+\frac{1}{2})^{2n}=\binom{2n}{0}+\binom{2n}{1}\frac{1}{2}+\dots$$

$$(1-\frac{1}{2})^{2n}=\binom{2n}{0}-\binom{2n}{1}\frac{1}{2}+\dots$$

And replace 2 by $\sqrt{2}$

Lecture 18, Oct. 14

18.1 Example. Given $n, m \in \mathbb{Z}^+$, find

$$\sum_{k=1}^{n} k^m = 1^m + 2^m + 3^m + \dots$$

Solution. For fixed $n \in \mathbb{Z}^+$, we can find a recursion formula for

$$S_m = \sum_{k=1}^{n} k^m$$

$$S_0 = \sum_{k=1}^{n} k^0 = n$$

$$S_1 = \sum_{k=1}^{n} k^1 = \frac{n(n+1)}{2} = \binom{n+1}{2}$$

Find

$$\sum_{k=1}^{n} (k+1)^{m+1} - k^{m+1}$$

in 2 ways.

1. $$\sum_{k=0}^{n} (k+1)^{m+1} - k^{m+1} = (n+1)^{m+1}$$

2. $$\begin{aligned}
&\sum_{k=0}^{n} (k+1)^{m+1} - k^{m+1} \\
=&\sum_{k=0}^{n} ((k^{m+1} + \binom{m+1}{1} k^m + \binom{m+1}{2} k^{m-1} + \dots + \binom{m+1}{m} k + \binom{m+1}{m+1}) - k^{m+1}) \\
=&\binom{m+1}{1} \sum_{k=0}^{n} k^m + \binom{m+1}{2} \sum_{k=0}^{n} k^{m-1} + \dots + \binom{m+1}{m} \sum_{k=0}^{n} k + \binom{m+1}{m+1} \sum_{k=0}^{n} 1
\end{aligned}$$

$$(n+1)^{m+1} = \binom{m+1}{1} \sum_{k=0}^{n} k^m + \binom{m+1}{2} \sum_{k=0}^{n} k^{m-1} + \dots + \binom{m+1}{m} \sum_{k=0}^{n} k + (n+1)$$

Thus

$$S_m = \frac{1}{m+1}((n+1)^{m+1} - \binom{m+1}{2} S_{m-1} - \dots - \binom{m+1}{m} S_1 - S_0 - 1)$$

18.2 Theorem. *Let $a, b, p, q \in \mathbb{R}$ (or $\mathbb{C}$) with $q \neq 0$ and let $m \in \mathbb{Z}$ Let $(X_n)_{n \geq m}$ be the sequence*

$$x_m = a, x_{m+1} = b, x_n = px_{n-1} + qx_{n-2} \text{ for } n \geq m+2$$

Let $f(x) = x^2 - px - q$ ($f(x)$ is called the characteristic polynomial for the recursion formula)

Suppose that $f(x)$ factors as

$$f(x) = (x-u)(x-v)$$

with $u, v \in \mathbb{R}$ (or $\mathbb{C}$) with $u \neq v$

Then there exist $A, B \in \mathbb{R}$ or $\mathbb{C}$ such that

$$x_n = Au^n + Bv^n$$

for all $n \geq m$

Proof. exercise □

18.3 Example. Let $(x_n)_{n \geq 0}$ be defined by

$$x_0 = 4, x_1 = -1, \ x_n = 3x_{n-1} + 10x_{n-2}$$

for $n \geq 2$.

Find a closed form formula for x_n

Solution. Let $f(x) = x^2 - 3x - 10 = (x-5)(x+2)$.

By the Linear Recursion Theorem, there exists $A, B \in \mathbb{R}$ such that

$$x_n = A5^n + B(-2)^n$$

for all $n \geq 0$.

To get $x_0 = A5^0 + B(-2)^0$, we need

$$A + B = 4. \tag{1}$$

To get $x_1 = A5^1 + B(-2)^1$, we need

$$5A - 2B = -1. \tag{2}$$

Solve 1 and 2 to get

$$A = 1, \ B = 3$$

Then

$$x_n = 5^n + 3(-2)^n$$

for all $n \geq 0$.

18.4 Example. There are n points on a circle around a disc. Each of the $\binom{n}{2}$ pairs of points is joined by a line segment. Suppose that no three of these line segment have a common point of intersection inside the disc.

Into how many regions is the disc divided by the line segments?

Solution. HINT

Suppose that we have l lines, each of which intersects the circle twice and intersects with the disc in a line segment.

Suppose these l line segments intersect at p points inside the disc. Suppose that no three of these line segment have a common point of intersection inside the disc. Into how many regions is the disc divided by the line segments?

Lecture 19, Oct. 17

Midterm today 7:00-8:50

RCH 207 Sec 2

RCH 211 Sec 1 A-O

RCH 309 Sec 1 P-Z

19.1 Definition. A **ring** (with identity) is a set R with two distinct elements $0, 1 \in R$ and two binary operations $+ : R^2 \to R$ and $\times : R^2 \to R$ where for $a, b \in R$ we write $+(a, b)$ as $a + b$, $\times(a, b)$ as $a \times b$ or $a \cdot b$ or ab, such that

1. $+$ is associative
$$\forall a, b, c \in R \ (a + b) + c = a + (b + c)$$
2. $+$ is commutative
$$\forall a, b \in R \ a + b = b + a$$
3. 0 is an identity under $+$
$$\forall a \in R \ a + 0 = a$$
4. every $a \in R$ has an inverse under $+$
$$\forall a \in R \, \exists b \in R \ a + b = 0$$
5. $\times$ is associative
$$\forall a, b, c \in R \ (ab)c = a(bc)$$
6. 1 is an identity under $\times$
$$\forall a \in R \ a \cdot 1 = a \text{ and } 1 \cdot a = a$$
7. $\times$ is distributive over $+$
$$\forall a, b, c \in R \ a(b + c) = ab + ac \text{ and } (a + b)c = ac + bc$$

A ring R is **commutative** when

8. $\times$ is commutative
$$\forall a, b \in R \ ab = ba$$

A **field** is commutative ring R such that

9. every nonzero $a \in R$ has an inverse under $\times$.
$$\forall 0 \neq a \in R \, \exists b \in R \ ab = 1$$

19.2 Theorem. *$\mathbb{Z}$ is commutative Ring. $\mathbb{Q}$ and $\mathbb{R}$ are fields.*

19.3 Example. $\mathbb{N}$ is not a ring (Axiom 4 does not hold)

$\mathbb{Z}$ is not a field (Axiom 9 does not work)

19.4 Example. The set of **integers modulo n**, denoted by $\mathbb{Z}_n$, is a ring for $n \in \mathbb{Z}$ with $n \geq 2$. Informally,

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$$

and addition and multiplication modulo n are denoted as follows:

for $a, b \in \mathbb{Z}_n$

$$a + b \in \mathbb{Z}_n \text{ is the remainder when } a + b \in \mathbb{Z} \text{ is divided by } n$$

$$ab \in \mathbb{Z}_n \text{ is the remainder when } ab \in \mathbb{Z} \text{ is divided by } n$$

In $\mathbb{Z}_6$:

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\times$	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	4	2
5	0	5	4	3	2	1

We shall see that $\mathbb{Z}_n$ is a field if and only if n is prime

19.5 Example. The field of **complex numbers** is the set

$$\mathbb{C} = \mathbb{R}^2 = \{(x, y) \mid x \in \mathbb{R}, y \in \mathbb{R}\}$$

and for $x, y \in \mathbb{R}$ we write

$$0 = (0,0), 1 = (1,0), i = (0,1), x = (x,0), iy = yi = (0,y), x + iy = (x,y)$$

and we define $+$ and $\times$ as follows

for $a, b, c, d \in R$

$$(a + ib) + (c + id) = (a, b) + (c, d) = (a + c, b + d) = (a + c) + i(b + d)$$

$$(a + ib)(c + id) = (ac - bd) + i(ad + bc)$$

Remark. Check that when $(a, b) \neq (0, 0)$, $a + ib$ has an inverse.

19.6 Example.

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{R}$$

is a ring.

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{R}$$

is a field.

$$\mathbb{Z}[\sqrt{3}i] = \{a + b\sqrt{3}i \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$$

is a ring.

$$\mathbb{Q}[\sqrt{3}i] = \{a + b\sqrt{3}i \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{C}$$

is a field.

19.7 Example. If R is a ring (usually commutative), the set of polynomials

$$f(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n$$

with coefficients $c_k \in R$ is a ring (under addition and multiplication of polynomials) which we denote by $R[x]$

19.8 Example. If R is a ring, the set of all $n \times n$ matrices $\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$ with entries $A_{kl} = a_{kl} \in R$ is a ring, which we denote by $M_n(R)$ (or $M_{n\times n}(R)$) (under addition and multiplication of matrices.)

Remark. Matrices

Lecture 20, Oct. 18

20.1 Axiom.

$$\forall x \, \forall y \, \forall z \ (x + y) + z = x + (y + z)$$

20.2 Axiom.

$$\forall x \, \forall y \ x + y = y + x$$

20.3 Axiom.

$$\forall x \ x + 0 = x$$

20.4 Axiom.

$$\forall x \, \exists y \ x + y = 0$$

20.5 Axiom.

$$\forall x \, \forall y \, \forall z \ (xy)z = x(yz)$$

20.6 Axiom.

$$\forall x \ 1x = x1 = x$$

20.7 Axiom.

$$\forall x \, \forall y \, \forall z \ x(y + z) = xy + xz \wedge (x + y)z = xz + yz$$

R is commutative when

20.8 Axiom.

$$\forall x \, \forall y \ xy = yx$$

R is a field when

20.9 Axiom.

$$\forall x \ (\neg x = 0 \to \exists y \ (xy = 1 \wedge yx = 1))$$

20.10 Definition. Let R be a ring. Let $a, b \in R$. If $ab = 1$ we sat that a is a **left inverse** of b and b is a **right inverse** of a

If $ab = ba = 1$, then we say that a and b are (2-sided) inverses of each other. We say that $a \in R$ is **invertible** or that a is a **unit** when a has a (2-sided) inverse b.

If $a \neq 0$ and $b \neq 0$ and $ab = 0$ then a and b are called **zero divisors**.

20.11 Theorem. ***Uniqueness of Identities and Inverses.*** *Let R be a ring.*

1. *The zero element is unique:*
   for all $e \in R$, if for all $x \in R$, $x + e = x$, then $e = 0$
2. *For all $a \in R$ the additive inverse of a is unique (which we denote by $-a$):*
   for all $a \in R$, for all $b, c \in R$, if $a + b = 0$ and $a + c = 0$ then $b = c$
3. *The identity element is unique.*
   for all $u \in R$, if for all $x \in R$ we have $x \cdot u = x$ and $u \cdot x = x$ then $u = 1$

4. *For every invertible $a \in R$, the multiplicative inverse of a is unique:*
   for all $a \in R$, for all $b, c \in R$, if $ab = ba = 1$ and $ac = ca = 1$, then $b = c$

Proof. 1. Let $e \in R$ be arbitrary. Suppose that for all $x \in R$, $x + e = x$. Then, in particular, $0 + e = 0$. Thus

$$\begin{aligned} e =& e + 0 \text{ by 20.3} \\ =& 0 + e \text{ by 20.2} \\ =& 0 \text{ as shown above} \end{aligned}$$

□

20.12 Exercise. Make a derivation to show that

$$\{20.2, 20.3\} \vDash \forall e \ (\forall x \ x + e = x \to e = 0)$$

20.13 Theorem. ***Some Additive Cancellation Properties.*** *Let R be a ring. Let $a, b, c \in R$ Then*

1. *if $a + b = a + c$ then $b = c$*
2. *if $a + b = a$ then $b = 0$*
3. *if $a + b = 0$ then $b = -a$*

Proof. 1. Suppose that $a + b = b + c$. Choose $d \in R$ so that $a + d = 0$ (by 20.4). Then

$$\begin{aligned} b =& b + 0 \text{ by 20.3} \\ =& b + (a + d) \text{ since } a + d = 0 \\ =& (b + a) + d \text{ by 20.1} \\ =& (a + b) + d \text{ by 20.2} \\ =& (a + c) + d \text{ since } a + b = a + c \\ =& (c + a) + d \text{ by 20.2} \\ =& c + (a + d) \text{ by 20.1} \\ =& c + 0 \text{ since } a + d = 0 \\ =& c \text{ by 20.3} \end{aligned}$$

□

20.14 Exercise. Make a derivation

20.15 Theorem. ***Some More basic Properties*** *Let R be a ring. Let $a, b \in R$ then,*

1. $0 \cdot a = 0$
2. $-(-a) = a$
3. $(-a)b = -(ab) = a(-b)$
4. $(-a)(-b) = ab$

5. $(-1)a = -a$

6. $a(b-c) = ab - ac$ *and* $(a-b)c = ac - bc$ *where* $x - y = x + (-y)$

Proof. 1. Choose $b \in R$ so that $0a + b = 0$

$$\begin{aligned} 0a =& (0+0)a \text{ by 20.3} \\ =& 0a + 0a \text{ by 20.3} \end{aligned}$$

$$\begin{aligned} 0a + b =& (0a + 0a) + b \text{ as shown above} \\ =& 0a + (0a + b) \text{ by 20.1} \end{aligned}$$

$$\begin{aligned} 0 =& 0a + 0 \text{ since } 0a + b = 0 \\ =& 0a \text{ by 20.3} \end{aligned}$$

□

20.16 Theorem. ***Multiplicative Cancellation*** *Let R be a ring. Let $a, b, c \in R$. Then if $ab = ac$ (or if $ba = ca$) then $a = o$ or a is a zero-divisor or $b = c$.*

Proof. Suppose $ab = ac$

Then $ab - ac = 0$, then $a(b-c) = 0$.

So either $a = 0$ or $b - c = 0$ or ($a \neq 0$ and $b - c \neq 0$) a is a zero-divisor ($b - c$ is a zero-divisor) □

Lecture 21, Oct. 19

21.1 Definition. A **total order** on a set S is a binary relation $\leq$ on S such that

1. Totality: for all $a, b \in S$, either $a \leq b$ or $b \leq a$
2. Antisymmetry: for all $a, b \in S$, if $a \leq b$ and $b \leq a$, then $a = b$
3. Transitivity; for all $a, b, c \in S$, if $a \leq b$ and $b \leq c$ then $a \leq c$

21.2 Example. The usual order $\leq$ is a total order on each of the sets: $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, and indeed on any subset of $\mathbb{R}$.

$\subseteq$ is a partial order on $P(S)$. If we define $a \leq b$ for $a, b \in \mathbb{N}$ to mean $a \mid b$ then $\leq$ is a partial order on $\mathbb{N}$

21.3 Definition. Given a total order $\leq$ on S, for $a, b \in S$, we define $a < b$ to mean ($a \leq b$ and $a \neq b$), $a \geq b$ to mean $b \leq a$, $a > b$ to mean $b < a$.

Remark. We could also define a total order on S to be a binary relation $<$ such that

1. for all $a, b \in S$ exactly one of the following holds:
$$a < b, a = b, b < a$$
2. for all $a, b, c \in S$ if $a < b$ and $b < c$ then $a < c$.

21.4 Definition. A **ordered field** is a field F with a total order $<$ such that

1. $<$ is compatible with $+$: for all $a, b, c \in F$
$$a < b \to a + c < b + c$$
2. $<$ is compatible with $\times$: for all $a, b \in F$,
$$0 < a \wedge 0 < b \to 0 < ab$$

21.5 Example. $\mathbb{Q}$ and $\mathbb{R}$ are ordered fields. Also $\mathbb{Q}[\sqrt{2}]$ is an ordered field.

21.6 Theorem. ***Properties of Ordered Fields*** *Let F be an ordered fields, and let $a, b, c \in F$.*

1. *If $a > 0$ then $-a < 0$ and if $a < 0$ then $-a > 0$*
2. *If $a > 0$ and $b < c$ then $ab < ac$*
3. *If $a < 0$ and $b < c$ then $ab < ac$*
4. *If $a \neq 0$ then $a^2 > 0$. In particular, $1 > 0$*
5. *if $0 < a < b$, then $0 < 1/b < 1/a$*

Proof.

1. Suppose $a > 0$, then

$$\begin{aligned} 0 &< a \\ 0 + (-a) &< a + (-a) \text{ since } < \text{ is compatible with } + \\ -a &< 0. \end{aligned}$$

   Suppose $a < 0$, then...

2. Suppose $a > 0$ and $b < c$, then

$$\begin{aligned} b &< c \\ b + (-b) &< c + (-b) \text{ since } < \text{ is compatible with } + \\ 0 &< c - b \\ 0 &< a(c - b) \text{ since } < \text{ is compatible with } \times \\ 0 &< ac - ab \\ 0 + ab &< (ac - ab) + ab \text{ since } < \text{ is compatible with } + \\ 0 + ab &< ac + (-ab + ab) \\ 0 + ab &< ac + (ab - ab) \\ 0 + ab &< ac + 0 \\ ab &< ac \end{aligned}$$

□

21.7 Example. When p is a prime numer we shall see that $\mathbb{Z}_p$ is a field. It is not possible to define an order which makes $\mathbb{Z}_p$ into an ordered field.

Proof. If $<$ was such an order then we would have

$$\begin{aligned} 1 &> 0 \\ -1 &< 0 \\ -1 = p - 1 = 1 + 1 + \cdots + 1 &> 0 \end{aligned}$$

By contradiction, such order does not exist. □

Similarly, it is not possible to define an order $<$ on $\mathbb{C}$ which makes $\mathbb{C}$ into an ordered field.

$$\begin{aligned} 1 &> 0 \\ -1 &< 0 \\ -1 = i^2 &> 0 \text{ by Property 21.6.4} \end{aligned}$$

21.8 Definition. Let F be an ordered field. For $a \in F$ we define the **absolute value** of a to be

$$|a| = \begin{cases} a & \text{if } a \geq 0 \\ -a & \text{if } a \leq 0 \end{cases}$$

21.9 Theorem. ***Properties of Absolute Value*** *Let F be an ordered field. Let $a, b \in F$. Then*

1. *Positive Definiteness*
$$|a| \geq 0 \wedge (|a| = 0 \leftrightarrow a = 0)$$
2. *Symmetry*
$$|a - b| = |b - a|$$
3. *Multiplicative*
$$|ab| = |a|\,|b|$$
4. *Triangle Inequality*
$$||a| - |b|| \leq |a - b| \leq |a| + |b|$$
5. *Approximation: for $b \geq 0$ and $x \in F$*
$$|x - a| < b \leftrightarrow a - b < x < a + b$$

Order Properties in $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$

21.10 Theorem. *In $\mathbb{Z}$,*

1. *for all $n \in \mathbb{Z}$*
$$n \in \mathbb{N} \leftrightarrow n \geq 0$$
2. *Discreteness: for all $n, kin\mathbb{Z}$,*
$$n \leq k \leftrightarrow n < k + 1$$
3. *Well Ordering Property: for every non-empty subset $S \subseteq \mathbb{Z}$, if S is bounded above in $\mathbb{Z}$, then S has a maximum element.*
4. *Well Ordering Property: for every non-empty subset $S \subseteq \mathbb{Z}$, if S is bounded below in $\mathbb{Z}$, then S has a minimum element.*

Remark. Well-Ordering is related to Induction.

Lecture 22, Oct. 21

Order Properties in $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$

22.1 Theorem. ***The Completeness Property in*** $\mathbb{R}$ *Every non-empty set $S \subseteq \mathbb{R}$ which is bounded above has a* ***supremum*** *(or least upper bound) in $\mathbb{R}$. Every non-empty set $S \subseteq \mathbb{R}$ which is bounded below has a* ***infimum*** *(or greatest lower bound) in $\mathbb{R}$*

In $S \subseteq R$, we say S is bounded above in $\mathbb{R}$ when there exists $b \in \mathbb{R}$ such that $b \geq x$ for every $x \in S$. Such a number b is called an ***upper bound*** *for S in $\mathbb{R}$. A* ***Supremum*** *for S is a number $b \in \mathbb{R}$ such that $b \geq x$ for every $x \in S$ and for all $c \in \mathbb{R}$, if $c \geq x$ for every $x \in \S$, then $b \leq c$.*

22.2 Theorem. ***Density of*** $\mathbb{Q}$ ***in*** $\mathbb{R}$ *For all $a, b \in \mathbb{R}$, if $a < b$ then there exists $c \in \mathbb{Q}$ such that $a < c < B$.*

22.3 Theorem. ***Order Properties in*** $\mathbb{Z}$

1. ***Natural numbers are non-negative.*** $\mathbb{N} = \{x \in \mathbb{Z} \mid x \geq 0\}$
2. ***Discreteness*** *for all $k, n \in \mathbb{Z}$, $k \leq n \leftrightarrow k < n + 1$*
3. ***Well Ordering Property of*** $\mathbb{Z}$ ***in*** $\mathbb{R}$*. Every nonempty set $S \subseteq \mathbb{Z}$ which is bounded above in $\mathbb{R}$ has a maximum element in S. Every nonempty set $S \subseteq \mathbb{Z}$ which is bounded below in $\mathbb{R}$ has a minimum element in S. In particular, every nonempty set $S \subseteq \mathbb{N}$ has a minimum number.*
4. *For every $x \in \mathbb{R}$, there exists $a \in \mathbb{Z}$ such that $a \leq x$. For every $x \in \mathbb{R}$, there exists $b \in \mathbb{Z}$ such that $x \leq b$.*
5. ***Floor and Ceiling Property*** *For every $x \in \mathbb{R}$ there exists a unique $n \in \mathbb{Z}$ which we denoted by $n = \lfloor x \rfloor$, such that $n \leq x$ and $n + 1 > x$. For every $x \in \mathbb{R}$ there exists a unique $m \in \mathbb{Z}$ which we denoted by $n = \lceil x \rceil$, such that $x \leq m$ and $x > m - 1$*
6. ***Monotone Sequence Property of*** $\mathbb{Z}$ *Let $m \in \mathbb{Z}$ and let $(x_n)_{n \geq m}$ be a sequence of integers (so each $x_n \in \mathbb{Z}$). If $x_{n+1} > x_n$ for all $n \geq m$, then for all $b \in \mathbb{R}$, there exists $n \geq m$ such that $x_n > b$. If $x_{n+1} < x_n$ for all $n \geq m$, then for all $b \in \mathbb{R}$, there exists $n \geq m$ such that $x_n < b$.*

Remark. If N has a total ordering $\leq$ and N has the property that every nonempty set $S \subseteq N$ has a minimum element, then we say that N is a well ordering set.

22.4 Exercise.
1. Show that for all $a \in \mathbb{Z}$, if $a \neq 0$ then $|a| \geq 1$
2. Show that the only units in $\mathbb{Z}$ are ± 1. Indeed show that for all $a, b \in \mathbb{Z}$, if $ab = 1$ then ($a = b = 1$ or $a = b = -1$)

Here ends Chapter 2: Rings Fields, Orders and Induction

Chapter 3: Factorization in $\mathbb{Z}$

22.5 Definition. For $a, b \in \mathbb{Z}$, we say a **divides** b, or a is a **factor** of b, or b is a **multiple** of a, and we write $a \mid b$, when

$$b = ak \text{ for some } k \in \digamma$$

22.6 Theorem.

1. *$1 \mid a$ for all $a \in \mathbb{Z}$*

2. $a \mid 1 \leftrightarrow a = \pm 1$
3. $0 \mid a \leftrightarrow a = 0$
4. $a \mid 0$ *for all* $a \in \mathbb{Z}$
5. $a \mid b \leftrightarrow |a| \mid |b|$
6. *if* $b \neq 0$ *and* $a \mid b$ *then* $|a| \leq |b|$
7. $a \mid a$
8. *if* $a \mid b$ *and* $b \mid a$ *then* $a = b$
9. *if* $a \mid b$ *and* $b \mid c$ *then* $a \mid c$
10. *if* $a \mid b$ *and* $a \mid c$ *then*
$$\forall x, y \in \mathbb{Z}\ a \mid (bx + cy)$$

Proof.

6. Suppose $b \neq 0$ and $a \mid b$. Choose $k \in \mathbb{Z}$ so that $b = ak$. If $k = 0$, then $b = ak = a0 = 0$. But $b \neq 0$, so $k \neq 0$. Since $k \neq 0$ we have $|k| \geq 1$. Since $b = ak$, we have $|b| = |ak| = |a|\,|k| \geq |a|\,1 = |a|$

□

Lecture 23, Oct. 24

Woman in Pure Math/Math Finance Lunch

Tuesday 12:30-1:20 MC5417

23.1 Theorem.

1. *if* $b \neq 0$ *and* $a \mid b$ *then* $|a| \leq |b|$
2. $a \mid a$
3. *if* $a \mid b$ *and* $b \mid a$ *then* $a = b$
4. *if* $a \mid b$ *and* $b \mid c$ *then* $a \mid c$
5. *if* $a \mid b$ *and* $a \mid c$ *then*
$$\forall x, y \in \mathbb{Z}\ a \mid (bx + cy)$$

Proof.

1. Let $a, b \in \mathbb{Z}$. Suppose $b \neq 0$ and $a \mid b$. Since $a \mid b$ we can choose $k \in \mathbb{Z}$ so that $b = ak$. Note that $k \neq 0$ because if $k = 0$ then $b = 0$ but $b \neq 0$. Since $k \neq 0$ we have $|k| \geq 1$. So we have
$$\begin{aligned} b &= ak \\ |b| &= |ak| \\ &= |a|\,|k| \\ &\geq |a| \cdot 1 \\ &= |a| \end{aligned}$$

2. Let $a \in \mathbb{Z}$. Since $a = a \cdot 1$, it follows that $a \mid a$.
$$\begin{aligned} \{\forall x\ x \cdot 1 = x\} &\vDash \forall x\ x \cdot 1 = x \\ &\vDash a \cdot 1 = a \\ &\vDash \exists x\ a \cdot x = a \end{aligned}$$

3. Let $a, b \in \mathbb{Z}$. Suppose $a \mid b$ and $b \mid a$. Choose $k \in \mathbb{Z}$ so that $b = ak$. Choose $l \in \mathbb{Z}$ sp that $a = bl$. Then $b = ak = (nl)k = b(lk)$
$$\begin{aligned} b - b(lk) &= 0 \\ b \cdot 1 - b(lk) &= 0 \\ b(1 - lk) &= 0 \end{aligned}$$
So $b = 0$ or $(1 - lk) = 0$ (Since $\mathbb{Z}$ has no zero divisors.)

   Case 1: Suppose $b = 0$, then $a = bl = 0 \cdot l = 0$, so we have $b = a = 0$, hence $b = \pm a$.

   Case 2: Suppose $1 - lk = 0$, then $lk = 1$ and so either $l = k = 1$ or $l = k = -1$. When $l = k = 1$, we have $b = ak = a \cdot 1 = a$, then $b = \pm a$. When $l = k = -1$, we have $b = ak = a(-1) = (-1)a = -a$, then $b = \pm a$.

   In all cases we have $b = \pm a$ as required.

4. *cdots*

5. Let $a, b, c \in \mathbb{Z}$. Suppose $a \mid b$ and $a \mid c$. Say $b = ak$ and $c = al$ with $k, l \in \mathbb{Z}$. Let $x, y \in \mathbb{Z}$.

$$\begin{aligned} bx + cy =& (ak)x + (al)y \\ =& a(kx) + a(ly) \\ =& a(kx + ly) \end{aligned}$$

$\therefore a \mid bx + cy$ as required.

□

Remark. $a \mid b$ means $\exists x\ b = ax$. $a \mid c$ means $\exists x\ c = ax$.

$$\begin{aligned} & [\exists x\ b = ax]_{b \mapsto bx+cy} \\ \equiv & [\exists u\ b = au]_{b \mapsto bx+cy} \\ \equiv & \exists u\ (bx + cy) = au \end{aligned}$$

$a \mid (bx + cy)$ means $\exists u\ (bx + cy) = au$

Remark. Recall that when $b \neq 0$, if $a \mid b$ then $|a| \leq |b|$. So b has finitely many divisors (and the greatest divisor is $|b|$).

23.2 Definition. For $a, b, d \in \mathbb{Z}$, we say that d is a **common divisor** of a and b when $d \mid a$ and $d \mid b$. When a and b are not both zero, there are only finitely many common divisor of a and b, and ± 1 are common divisors, so a and b do have a greatest common divisor and we denote it by $gcd(a, b)$.

For convenience, we also write $gcd(0, 0) = 0$

23.3 Theorem. ***(Properties of the GCD)*** *Let $a, b, c \in \mathbb{Z}$.*

1. $gcd(a, b) = gcd(b, a)$
2. $gcd(a, b) = gcd(|a|, |b|)$
3. *if $a \mid b$ then $gcd(a, b) = |a|$, in particular, $gcd(a, 0) = |a|$*
4. $gcd(a, b) = gcd(a + tb, b)$ *for all $t \in \mathbb{Z}$.*
5. *if $a = qb + r$ where $q, r \in \mathbb{Z}$, then $gcd(a, b) = gcd(b, r)$*

Proof. 4 To show that $gcd(a, b) = gcd(a + tb, b)$ we shall show that the common divisor of a and b is exactly the same as the common divisor of $a + tb$ and b.

Let $a, b, t \in \mathbb{Z}$. Let $d \in \mathbb{Z}$. Suppose $d \mid a$ and $d \mid b$ then $d \mid ax + by$ for all $x, y \in \mathbb{Z}$. In particular, $d \mid (a \cdot 1 + bt)$, so $d \mid (a + td)$. Thus $d \mid (a + tb)$ and $d \mid b$.

Conversely, suppose $d \mid (a + tb)$ and $d \mid b$. Then $d \mid (a + tb)x + by$ for all $x, y \in \mathbb{Z}$. In particular, $d \mid (a + tb) \cdot 1 + b \cdot (-1)$, so $d \mid a$. Thus $d \mid a$ and $d \mid a$.

□

Lecture 24, Oct. 25

24.1 Theorem (The Division Algorithm)**.** *Let $a, b \in \mathbb{Z}$ with $b \neq 0$. There exist unique $q, r \in \mathbb{Z}$ such that $a = qb + r$ and $0 \leq r < |b|$*

Since $b \neq 0$, either $b > 0$ or $b < 0$.

Case 1: Suppose $b > 0$. Let $q = \lfloor a/b \rfloor$ ($q \leq a/b$ and $q + 1 > a/b$). Let $r = a - qb$.

Proof. Since $q \leq a/b$ we have

$$\begin{aligned} qb &\leq a \\ 0 &\leq a - qb \\ 0 &\leq r \end{aligned}$$

Since $q + t > a/b$

$$\begin{aligned} (q+1)b &> a \\ qb + b &> a \\ b &> a - qb \\ b &> r \end{aligned}$$

Thus $r < b = |b|$ □

Another proof. Suppose $b > 0$ and $a \geq 0$. Consider the sequence

$$0b, 11b, 2b, 3b, \cdots$$

Eventually, the terms kb exceed a. Choose $q \geq 0$ so that $qb \leq a$ and $(q + 1)b > a$. (In fact, we choose $q = max(S)$ where $S = \{t \geq - \mid tb \leq a\}$ and we have $S \neq \emptyset$ since $0 \in S$ and S is bounded above by $a + 1$)

Then we have

$$\begin{aligned} qb &\leq a \\ 0 \leq a - qb \\ 0 &\leq r \end{aligned}$$

and

$$\begin{aligned} (q+1)b &> a \\ qb + b &> a \\ b &> a - qb \\ b &> r \end{aligned}$$

So $r < b = |b|$. □

Case 2: Suppose $b < 0$. Let $c = -b$ so $c > 0$. Using the result of Case 1 we can choose $p, r \in \mathbb{Z}$ so that $a = pc + r$ and $0 \leq r < c$. Then $a = -pb + r$. So we can choose $q = -p$ to get $a = qb + r$ and $0 \leq r < |b|$.

Proof of Uniqueness. Suppose that

$$a = qb + r \text{ with } 0 \leq r < |b|$$

and Suppose that

$$a = pb + s \text{ with } 0 \leq r < |b|$$

Suppose, for a contradiction, that $r \neq s$. Then $0 \leq r < s < |b|$. Since $r < s$ we have $s - r > 0$ Since $r \geq 0$ and $s < |b|$ we have $s - r \leq s < |b|$. Thus $0 < s - r < |b|$. Since $a = qb + r$ and $a = pb + s$,

$$\begin{aligned} qb + r &= pb + s \\ qb - pb &= s - r \\ (q - p)b &= s - r \end{aligned}$$

Thus $b \mid (s - r)$

...

Leads to contradiction.

Thus $r = s$.

...

Then $p = q$ □

24.2 Theorem (The Euclidean Algorithm with Back-substitution)**.** *Let $a, b \in \mathbb{Z}$, and let $d = gcd(a, b)$. Then there exist $s, t \in \mathbb{Z}$ such that $as + bt = d$.*

The proof of the theorem provides an **Algorithm** (that is a systematic procedure) called the **The Euclidean Algorithm** for computing $d = gcd(a, b)$ and an algorithm, called **Back-Substitution**, for finding $s, t \in \mathbb{Z}$ such that $as + bt = d$.

Lecture 25, Oct. 26

25.1 Theorem (The Euclidean Algorithm with Back-substitution)**.** *Let $a, b \in \mathbb{Z}$, and let $d = gcd(a, b)$. Then there exist $s, t \in \mathbb{Z}$ such that $as + bt = d$.*

The proof of the theorem provides an **Algorithm** (that is a systematic procedure) called the **The Euclidean Algorithm** for computing $d = gcd(a, b)$ and an algorithm, called **Back-Substitution**, for finding $s, t \in \mathbb{Z}$ such that $as + bt = d$.

Proof. If $b \mid a$, then $gcd(a, b) = |b|$ and we can take $s = 0$ and $t = \pm 1$ to get $as + bt = d$.

Suppose $b \nmid a$.

Then apply the Division Algorithm repeatedly to get

$$a = q_1 b + r_1$$

$$b = q_2 r_1 + r_2$$

$$r_1 = q_3 r_2 + r_3$$

$$\cdots$$

$$r_{n-3} = q_{n-1} r_{n-2} + r_{n-1}$$

$$r_{n-2} = q_n r_{n-1} + r_n$$

$$r_{n-1} = q_{n+1} r_n + 0$$

$$gcd(a, b) = gcd(b, r_1) = gcd(r_1, r_2) = \cdots = gcd(r_n, 0) = r_n$$

Thus $d = gcd(a, b) = r_n$, the last non-zero remainder.

We have

$$\begin{aligned} d = r_n =& r_{n-2} - q_n r_{n-1} \\ =& S_0 r_{n-2} + S_1(r_{n-3} - q_{n-1} r_{n-2}) \text{ where } S_0 = 1 \text{ and } S_1 = -q_n \\ =& S_1 r_{n-3} + (S_0 - q_{n-1} S_1) r_{n-2} \\ =& S_1 r_{n-3} + S_2 r_{n-2} \text{ where } S_2 = S_0 - q_{n-1} S_1 \end{aligned}$$

We have a sequence $(S_l)_{l \geq 0}$ by $S_0 = 1$, $S_1 = -q_n$ and

$$S_{l+1} = S_{l-1} - q_{n-l} S_l$$

We claim that

$$d = r_k = S_{l-1} r_{n-l-1} + S_l r_{n-l}.$$

Proof by induction: $\cdots$. □

25.2 Example. Let $a = 5151$ and $b = 1632$. Find $d = gcd(a, b)$ and find $s, t \in \mathbb{Z}$ such that $as + bt = d$.

Solution.

$$5151 = 1632 \cdot 3(q_1) + 255$$
$$1632 = 255 \cdot 6(q_2) + 102$$
$$255 = 102 \cdot 2(q_3) + 51$$
$$102 = 51 \cdot 2 + 0$$

Thus $d = gcd(a, b) = 51$

$$S_0 = 1$$
$$S_1 = -q_3 = -2$$
$$S_2 = S_0 - S_1 q_2 = 13$$
$$S_3 = S_1 - S_2 q_1 = -41$$

So we can take $s = 13$ and $t = -41$ to get $as + bt = d$

25.3 Example. Let $a = 754$ and $b = -3973$. Find $d = gcd(a, b)$ and find $s, t \in \mathbb{Z}$ such that $as + bt = d$.

Solution.

$$3973 = 754 \cdot 5(q_1) + 203$$
$$754 = 203 \cdot 3(q_2) + 145$$
$$203 = 145 \cdot 1(q_3) + 58$$
$$145 = 58 \cdot 2(q_4) + 29$$
$$58 = 29 \cdot 2 + 0$$

Thus $d = gcd(a, b) = 29$

$$S_0 = 1$$
$$S_1 = -q_4 = -2$$
$$S_2 = S_0 - S_1 q_3 = 3$$
$$S_3 = S_1 - S_2 q_2 = -11$$
$$S_4 = S_2 - S_3 q_1 = 58$$

Thus $(3973)(-11) + (754)(58) = 29$

Thus we can take $s = 58$ and $t = 11$ to get $as + bt = d$

25.4 Theorem (More Properties of GCD)**.** *Let $a, b, c \in \mathbb{Z}$*

1. *if $c \mid a$ and $c \mid b$ then $c \mid gcd(a, b)$*
2. *there exist $x, y \in \mathbb{Z}$ such that $ax + by = c$ iff $gcd(a, b) \mid c$*
3. *there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$ iff $gcd(a, b) = 1$*
4. *if $d = gcd(a, b) \neq 0$ (which is the case unless $a = b = 0$) then $gcd(a/d, b/d) = 1$*

5. *if* $a \mid bc$ *and* $gcd(a, b) = 1$ *then* $a \mid c$

Proof. 5. Let $a, b, c \in \mathbb{Z}$. Suppose $a \mid bc$ and $gcd(a, b) = 1$. Since $a \mid bc$, choose $k \in \mathbb{Z}$ such that $bc = ak$. Since $gcd(a, b) = 1$, we can choose $s, t \in \mathbb{Z}$ such that $as + bt = 1$. Then $c = c \cdot 1 = c \cdot (as + bt) = acs + bct = acs + akt = a(cs + kt)$. So $a \mid c$

□

Lecture 26, Oct. 28

26.1 Theorem (Properties of GCD)**.** *Let $a, b, c \in \mathbb{Z}$*

1. *if $c \mid a$ and $c \mid b$ then $c \mid gcd(a, b)$*
2. *there exist $x, y \in \mathbb{Z}$ such that $ax + by = c$ iff $gcd(a, b) \mid c$*
3. *there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$ iff $gcd(a, b) = 1$*
4. *if $d = gcd(a, b) \neq 0$ (which is the case unless $a = b = 0$) then $gcd(a/d, b/d) = 1$*
5. *if $a \mid bc$ and $gcd(a, b) = 1$ then $a \mid c$*

Proof. 5. Let $a, b, c \in \mathbb{Z}$. Suppose $a \mid bc$ and $gcd(a, b) = 1$. Since $a \mid bc$, choose $k \in \mathbb{Z}$ such that $bc = ak$. Since $gcd(a, b) = 1$, we can choose $s, t \in \mathbb{Z}$ such that $as + bt = 1$. Then $c = c \cdot 1 = c \cdot (as + bt) = acs + bct = acs + akt = a(cs + kt)$. So $a \mid c$

□

26.2 Definition (Prime)**.** Let $n \in \mathbb{Z}$. We say that n is a **prime** when $n > 1$ and n has no factors $a \in \mathbb{Z}$ with $1 < a < n$.

We say n is composite when $n > 1$ and n does have a factor $a \in \mathbb{Z}$ with $1 < a < n$.

Note. If $n > 1$ and $n = ab$ with $1 < a < n$ then we also have $1 < b < n$.

26.3 Theorem. *Every composite number n has a prime factor p with $p \leq \sqrt{n}$.*

Proof. We claim that every integer $n \geq 2$ has a prime factor.

Let $n \geq 2$. Suppose, inductively, that for every $a \in \mathbb{Z}$ with $2 \leq a < n$, a has a prime factor. If n is prime, then since $n \mid n$, n has a prime factor. Suppose n is not prime, say $n = ab$ with $1 < a < n$ and $1 < b < n$. Since $1 < a < n$ we have $2 \leq a < n$, so a has a prime factor, say $p \mid a$ and p is prime. Since $p \mid a$ and $a \mid n$ then $p \mid n$, so p has a prime factor.

By induction, every integer $n \geq 2$ does have a prime factor.

Let $n \geq 2$ be arbitrary. Suppose n is composite, say $n = ab$ with $1 < a < n$ and $1 < b < n$. Say $a \leq b$ (the case $b \leq a$ is similar). Note that $a \leq \sqrt{n}$ since if $a > \sqrt{n}$ then we have $n = ab \geq aa > \sqrt{n}\sqrt{n} = n$ which is not possible. Since $1 < a < n$, we have $a \geq 2$. So a has a prime factor. Let p be a prime factor of a. Since $p \mid a$ and $a \mid n$ then $p \mid n$. Since $p \mid a$ we have $p \leq a \leq \sqrt{n}$. □

Note. There is a method for listing all prime numbers $p \leq n$, where $n \geq 2$ is a given integer, called the **Sieve of Eratosthenes**.

It works as follows:

We begin by listing all the numbers from 1 to n. We cross off the number 1. We circle the smallest remaining number (namely $p_1 = 2$). Cross off all the other multiples of $p_1 = 2$ (they are composites). Circle the smallest remaining number (namely $p_2 = 3$). Cross off all the other multiples of $p_2 = 3$ (they are composites). Repeat this procedure until we have circled a prime p_l with $p_l \geq \sqrt{n}$ and crossed off the other multiples of p_l.

Note that after we have circled $p_1, p_2, \cdots, p_k$ and crossed off all their multiples, the smallest remaining numbers p_{k+1} must be prime since if it were composite it would have a prime factor $p < p_{k+1}$, but we have already found and crossed off all multiples of all primes p with $p < p_{k+1}$.

Also note that after we have found $p_l \geq \sqrt{n}$ and circled all multiples, all reaming numbers $m \leq n$ are prime since if $m \leq n$ is composite, then m has a prime factor with $p \leq \sqrt{m} \leq \sqrt{n}$, but we have already crossed off all multiples of all such primes.

26.4 Example. Find all primes $p \leq 100$

Solution.

(2), (3), (5), (7), ~~9~~, (11), (13), ~~15~~, (17), (19), ~~21~~, (23), ~~25~~, ~~27~~, (29), (31), ~~33~~, ~~35~~, (37), ~~39~~, (41), (43), ~~45~~, (47), ~~49~~

~~51~~, (53), ~~55~~, ~~57~~, (59), (61), ~~63~~, ~~65~~, (67), ~~69~~, (71), (73), ~~75~~, ~~77~~, (79), ~~81~~, (83), ~~85~~, ~~87~~, (89), ~~91~~, ~~93~~, ~~95~~, (97), ~~99~~

26.5 Theorem (The Infinitude of Primes)**.** *There are infinitely many primes.*

Proof. Suppose, for a contradiction, that there are finitely many primes, say $p_1, p_2, \cdots, p_l$, consider the number

$$n = p_1 p_2 \cdots p_l + 1.$$

Since n has a prime factor, we know that one of the primes is a factor of n, say $p_k \mid n$. So $gcd(p_k, n) = p_k$

But

$$\begin{aligned} gcd(p_k, n) =& gcd(n, p_k) \\ =& gcd(p_1 p_2 \cdots p_l + 1, p_k) \\ =& gcd(1, p_k) \\ =& 1 \end{aligned}$$

□

Lecture 27, Oct. 31

Note. There exist arbitrary large gaps between prime numbers.

27.1 Theorem (Bertrand's postulate)**.** *For every $n \in \mathbb{Z}^+$ there is a prime p with $n < p \leq 2n$*

27.2 Theorem (Dirichlet's Theorem on Primes in Arithmetic Progression)**.** *Let $a, b \in \mathbb{Z}^+$ with $gcd(a, b) = 1$. Then there exists infinitely many primes p of the form $p = a + tb$ for some $t \in \mathbb{Z}$. In other words, there exist infinitely many primes in the sequence*

$$a, a + b, a + 2b, a + 3b, \cdots$$

27.3 Theorem (The Prime Number Theorem)**.** *For $x \in \mathbb{R}$ let $\pi(x)$ denote the number of primes p with $p \leq x$. Then*

$$\pi(x) \ \frac{x}{lnx}$$

which means that

$$\lim_{x\to\infty} \frac{\pi(x)}{x/lnx} = 1$$

27.4 Conjecture (n^2 Conjecture)**.** For all $n \in \mathbb{Z}^+$ there exists a prime p with $n^2 < p < (n + 1)^2$

27.5 Conjecture ($n^2 + 1$ Conjecture)**.** There are infinitely many primes of the form $p = n^2 + 1$ for some $n \in \mathbb{Z}$

27.6 Conjecture (Mersenne Primes Conjecture)**.** There exist infinitely many primes of the form $p = 2^n - 1$ for some $n \in \mathbb{Z}^+$ (such primes are called Mersenne Primes).

27.7 Exercise. If $2^n - 1$ is prime, then n is prime.

27.8 Conjecture (Fermat Primes Conjecture)**.** There are only finitely many primes of the form $p = 2^n + 1$ with $n \in \mathbb{Z}^+$ (such primes are called Fermat primes).

27.9 Exercise. If $2^n + 1$ is prime then $n = 2^k$ for some $k \in \mathbb{N}$

27.10 Conjecture (Twin Primes Conjecture)**.** There exist infinitely many primes p such that $p + 2$ is also prime. Such primes p and $p + 2$ are called twin primes.

27.11 Conjecture (Goldbach's Conjecture)**.** Every even number $n \geq 2$ is a sum of two primes.

27.12 Theorem (Unique Prime Factorization)**.** *Every integer $n \geq 2$ can be expressed uniquely in the form*

$$n = \prod_{i=1}^{l} p_i = p_1 p_2 \cdots p_l$$

for some $l \in \mathbb{Z}^+$ and some primes $p_1, p_2, \cdots, p_l$ with $p_1 \leq p_2 \leq \cdots \leq p_l$.

Proof. First we show existence. Let $n \geq 2$. Suppose, inductively, that every integer k with $2 \leq k < n$ can be written (uniquely) in the required form. If n is prime then $n = p_1$ with $p_1 = n$.

Suppose n is composite, say $n = ab$ with $1 < a < n$ and $1 < b < n$. Since $2 \leq a < n$ and $2 \leq n < n$ we can write

$$a = \prod_{i=1}^{l} p_i$$

and

$$b = \prod_{j=1}^{m} q_j$$

with $l, m \in \mathbb{Z}$ and the q_j, p_i are primes.

Thus

$$\begin{aligned} n =& ab \\ =& p_1 p_2 \cdots p_l q_1 q_2 \cdots q_m \\ =& r_1 r_2 \cdots r_{l+m} \end{aligned}$$

where the $(l+m)-$tuple $(r_1, r_2, \cdots, r_{l+m})$ is obtained by rearranging the entries of the

$$\text{(l+m)-tuple } (p_1, p_2, \cdots, p_l, q_1, q_2, \cdots, q_m)$$

into non-decreasing order.

Next we prove uniqueness. We need to show that if $n = p_1 p_2 \cdots p_l$ and $n = q_1 q_2 \cdots q_m$ where $l, m \in \mathbb{Z}^+$ and the p_i and q_j are primes with $p_1 \leq p_2 \leq \cdots \leq p_l$ and $q_1 \leq q_2 \leq \cdots q_m$, then $l = m$ and $p_i = q_i$ for all i.

Suppose $n = p_1 p_2 \cdots p_l = q_1 q_2 \cdots q_m$ as above. Since $n = p_1 p_2 \cdots p_l$ we have $p_1 \mid n$. Since $n = q_1 q_2 \cdots q_m$ we have $p_1 \mid q_1 q_2 \cdots q_m$. It follows that $p_1 \mid q_k$ for some k with $1 \leq k \leq m$. Say $p_1 \mid q_k$. Since q_k is prime, its only positive divisors are 1 and q_k. Since $p_1 \neq 1$, so $p_1 = q_k$. Similarly, $q_1 = p_j$ for some j with $1 \leq j \leq l$. Since $p_1 = q_k \geq q_1 = p_j \geq p_1$, so we must have $p_1 = p_j = q_1$. $\square$

Lecture 28, Nov. 1

28.1 Theorem (Unique Prime Factorization)**.** *Every integer $n \geq 2$ can be expressed uniquely in the form*

$$n = \prod_{i=1}^{l} p_i = p_1 p_2 \cdots p_l$$

for some $l \in \mathbb{Z}^+$ and some primes $p_1, p_2, \cdots, p_l$ with $p_1 \leq p_2 \leq \cdots \leq p_l$.

Proof. First we show existence. Let $n \geq 2$. Suppose, inductively, that every integer k with $2 \leq k < n$ can be written (uniquely) in the required form. If n is prime then $n = p_1$ with $p_1 = n$.

Suppose n is composite, say $n = ab$ with $1 < a < n$ and $1 < b < n$. Since $2 \leq a < n$ and $2 \leq n < n$ we can write

$$a = \prod_{i=1}^{l} p_i$$

and

$$b = \prod_{j=1}^{m} q_j$$

with $l, m \in \mathbb{Z}$ and the q_j, p_i are primes.

Thus

$$\begin{aligned} n =& ab \\ =& p_1 p_2 \cdots p_l q_1 q_2 \cdots q_m \\ =& r_1 r_2 \cdots r_{l+m} \end{aligned}$$

where the $(l+m)-$tuple $(r_1, r_2, \cdots, r_{l+m})$ is obtained by rearranging the entries of the

$$\text{(l+m)-tuple } (p_1, p_2, \cdots, p_l, q_1, q_2, \cdots, q_m)$$

into non-decreasing order.

Next we prove uniqueness. We need to show that if $n = p_1 p_2 \cdots p_l$ and $n = q_1 q_2 \cdots q_m$ where $l, m \in \mathbb{Z}^+$ and the p_i and q_j are primes with $p_1 \leq p_2 \leq \cdots \leq p_l$ and $q_1 \leq q_2 \leq \cdots q_m$, then $l = m$ and $p_i = q_i$ for all i.

Suppose $n = p_1 p_2 \cdots p_l = q_1 q_2 \cdots q_m$ as above. Since $n = p_1 p_2 \cdots p_l$ we have $p_1 \mid n$. Since $n = q_1 q_2 \cdots q_m$ we have $p_1 \mid q_1 q_2 \cdots q_m$. It follows that $p_1 \mid q_k$ for some k with $1 \leq k \leq m$. Say $p_1 \mid q_k$. Since q_k is prime, its only positive divisors are 1 and q_k. Since $p_1 \neq 1$, so $p_1 = q_k$. Similarly, $q_1 = p_j$ for some j with $1 \leq j \leq l$. Since $p_1 = q_k \geq q_1 = p_j \geq p_1$, so we must have $p_1 = p_j = q_1$.

Since $p_1 p_2 \cdots p_l = q_1 q_2 \cdots q_m$ and $q_1 = p_1 \neq 0$, we have $p_2 p_3 \cdots p_l = q_2 q_3 \cdots q_m$. A similar argument shows that $p_2 = q_2$.

Suppose for a contradiction, that $l \neq m$, say $l < m$. By repeating the above argument, we eventually obtain

$$p_l = q_l \cdots q_m$$

then $p_l = q_l$ then $1 = q_{l+1} \cdots q_m$. But each $q_j \geq 2$ so $q_{l+1} \cdots q_m \geq 2$, so we have a desired contradiction, hence $m = l$.

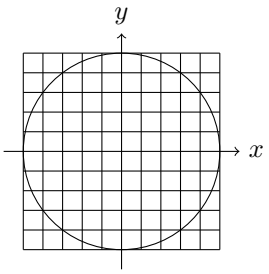
Thus repeating the above argument gives

$$p_1 = q_1, p_2 = q_2, \cdots, p_l = q_l = q_m.$$ □

28.2 Definition (Diophantine Equation)**.** A Diophantine Equation is a polynomial equation where the variables represent integers.

28.3 Example. Solve

$$x^2 + y^2 = 25$$



28.4 Example. Solve

$$x^2 + y^2 = n$$

in $\mathbb{Z}[i]$ where $i^2 = -1$

28.5 Example. A Linear Diophantine Equation is an equation of the form

$$ax + by = c$$

where $a, b, c \in \mathbb{Z}$ with $(a, b) \neq 0$

28.6 Example (Pell's Equation)**.** Solve

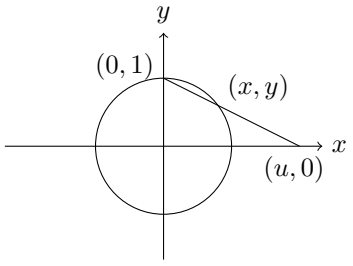
$$x^2 - dy^2 = \pm 1$$

28.7 Example (Pythagorean Triples)**.** Solve

$$x^2 + y^2 = z^2$$

$$x^2 + y^2 + z^2 = w^2$$

Stereographic Projection



Lecture 29, Nov. 2

29.1 Theorem (Linear Diophantine Equation Theorem)**.** *Let $a, b, c \in \mathbb{Z}$ with $(a, b) \neq (0, 0)$. Let $d = gcd(a, b)$. Consider the equation*

$$ax + by = c.$$

The equation has a solution (x, y) with $x, y \in \mathbb{Z}$ if and only if $d \mid c$. In this case if (u, v) is a solution with $u, v \in \mathbb{Z}$, then the general solution is

$$(x, y) = (u, v) + k(-\frac{b}{d}, \frac{a}{d})$$

Proof. Suppose that the equation has a solution. Choose $x, y \in \mathbb{Z}$ so that $ax + by = c$. Since $d \mid a$ and $d \mid b$, $d \mid ax + by$, so $d \mid c$.

Conversely, Suppose that $d \mid c$, say $c = dl$. Use EA with BS to obtain $s, t \in \mathbb{Z}$ such that

$$as + bt = d$$

. Then

$$asl + btl = dl = c.$$

So we have

$$ax + by = c$$

with $x = sl$ and $y = tl$

Suppose that $d \mid c$ and suppose that $u, v \in \mathbb{Z}$ with $au + bv = c$. We need to show that

1. for all $k \in \mathbb{Z}$, if we let $(x, y) = (u, v) + k(-\frac{b}{d}, \frac{a}{d})$, then $ax + by = c$
2. for all $x, y \in \mathbb{Z}$, if $ax + by = c$, then there exists $k \in \mathbb{Z}$ such that $(x, y) = (u, v) + k(-\frac{b}{d}, \frac{a}{d})$

To prove 1, let $k \in \mathbb{Z}$ and let $(x, y) = (u, v) + k(-\frac{b}{d}, \frac{a}{d})$, that is $x = u - k\frac{b}{d}$ and $y = v + k\frac{a}{d}$. Then

$$\begin{aligned} ax + by =& a(u - k\frac{b}{d}) + b(v + k\frac{a}{d}) \\ =& au + bv - k\frac{ab}{d} + k\frac{ab}{d} \\ =& au + bv \\ =& c \end{aligned}$$

To prove 2, let $x, y \in \mathbb{Z}$. Suppose $ax + by = c$. Since $ax + by = c$ and $au + bv = c$,

$$a(x - u) + b(y - v) = 0$$

so

$$\frac{a}{d}(x - u) = -\frac{b}{d}(y - v)$$

and note that $\frac{a}{d} \in \mathbb{Z}$ and $\frac{b}{d} \in \mathbb{Z}$. It follows that

$$\frac{a}{d} \mid (y - v).$$

Choose $k \in \mathbb{Z}$ so that

$$y - v = k\frac{a}{d}.$$

Since $y - v = k\frac{a}{d}$ and

$$\frac{a}{d}(x-u) = -\frac{b}{d}(y-v)$$

we have

$$\frac{a}{d}(x-u) = -\frac{b}{d}k\frac{a}{d}$$

so

$$x - u = -k\frac{b}{d}.$$

So we have

$$x = u - k\frac{b}{d} \text{ and } y = v + k\frac{a}{d}$$ □

29.2 Theorem (Unique Prime Factorization)**.** *Every integer $n \geq 2$ can be expressed uniquely in the form*

$$n = \prod_{i=1}^{l} p_i = p_1 p_2 \cdots p_l$$

for some $l \in \mathbb{Z}^+$ and some primes $p_1, p_2, \cdots, p_l$ with $p_1 \leq p_2 \leq \cdots \leq p_l$.

Alternatively, every integer $n \geq 2$ can be written uniquely in the form

$$n = \prod_{i=1}^{l} p_i^{k_i}$$

with $l \in \mathbb{Z}^+$ and p_i are distinct primes with $p_1 < p_2 < \cdots < p_l$ and each $k_i \in \mathbb{Z}^+$.

Alternatively, given an integer $n \geq 1$ if every prime factor of n is included in the set $\{p_1, p_2, \cdots, p_l\}$ where the p_i are distinct primes, then n can be written uniquely in the form

$$n = \prod_{i=1}^{l} p_i^{k_i}$$

with each $k_i \in \mathbb{N}$

When

$$n = \prod_{i=1}^{l} p_i^{k_i}$$

where the p_i are distinct primes and each $k_i \in \mathbb{N}$, the positive divisor of n are the integers a of the form

$$a = \prod_{i=1}^{l} p_i^{d_i}$$

such that $0 \leq d \leq k_i$ for all indices i.

29.3 Theorem. *The number of positive divisors of n is*

$$\tau(n) = \prod_{i=1}^{l}(k_i + 1)$$

The sum of the positive divisors of n is

$$\sigma(n) = \prod_{i=1}^{l} \frac{p_i^{n+1} - 1}{p - 1}.$$

29.4 Theorem. *The product of all the positive divisors of n is*

$$p(n) = n^{\tau(n)/2}$$

Proof. exercise □

29.5 Definition. For $n = \prod_{i=1}^{l} p_i^{k_i}$ the exponent of p in n

$$\begin{cases} k_i & \text{if } p = p_i \\ 0 & \text{if } p \notin \{p_1, p_2, \cdots, p_l\} \end{cases}$$

Lecture 30, Nov. 4

30.1 Definition. For $a, b \in \mathbb{Z}$, if $a \neq 0$ and $b \neq 0$ then $lcm(a, b)$ is the smallest $m \in \mathbb{Z}^+$ such that $a \mid m$ and $b \mid m$, and $lcm(a, 0) = lcm(0, a) = 0$.

30.2 Theorem. *Let $a, b \in \mathbb{Z}$. Write*

$$a = \prod_{i=1}^{m} p_i^{k_i}$$

and

$$b = \prod_{i=1}^{m} p_i^{l_i}$$

then

$$gcd(a, b) = \prod_{i=1}^{m} p_o^{min(k_i, l_i)}$$

and

$$lcm(a, b) = \prod_{i=1}^{m} p_o^{max(k_i, l_i)}$$

and

$$gcd(a, b)lcm(a, b) = ab$$

Here ends Chapter 3: Factorization in $\mathbb{Z}$

Chapter 4: Integers Modulo n

Recall that, informally, $\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$ and we add and multiply by adding and multiplying in $\mathbb{Z}$ then finding the remainder after dividing by n.

30.3 Definition (Partition)**.** A partition of a set S is a set P of non-empty disjoint sets whose union is S, that is for all $A \in P$, $A \neq \emptyset$, for all $A, B \in P$, if $A \neq B$ then $A \cap B = \emptyset$ and

$$\bigcup P = \bigcup_{A \in P} A = S$$

or equivalently for all $A \in P$ we have $A \subseteq S$ and for all $a \in S$ we have $a \in A$ for some $A \in P$

30.4 Definition (Equivalence Relation)**.** A equivalence relation on a set S is a binary relation $\sim$ on s such that

1. Reflexivity: for all $a \in S$, $a \sim a$
2. Symmetry: for all $a, b \in S$, if $a \sim b$ then $b \sim a$
3. Transitivity: for all $a, b \in S$, if $a \sim b$ and $b \sim c$ then $a \sim c$

30.5 Definition (Equivalence Class)**.** Given an equivalence relation $\sim$ on a set S, for $a \in S$, the equivalence class of a (in S under $\sim$) is the set

$$[a] = \{x \in S \mid x \sim a\}$$

30.6 Theorem (Equivalence Classes Form a Partition)**.** *Let S be a set. Let $\sim$ be an equivalence relation on S. Then*

1. *for all* $a \in S$ *we have* $a \in [a]$
2. *for all* $a, b \in S$ *we have* $[a] = [b] \Leftrightarrow a \sim b \Leftrightarrow a \in [b] \Leftrightarrow b \in [a]$
3. *for all* $a, b \in S$, *if* $[a] \neq [b]$ *then* $[a] \cap [b] = \emptyset$

It follows that

$$P = \{[a] \mid a \in S\}$$

is a partition of S

Proof. 1. for $a \in S$ we have $a \in [a]$ since $a \sim a$

2. Let $a, b \in S$. Suppose $[a] = [b]$. Then $a \in [a]$ and $[a] = [b]$ so $a \in [b]$ so $a \sim b$. Note that $a \in [b] \Leftrightarrow a \sim b$. Suppose that $a \in [b]$ then $a \sim b$. If $x \in [a]$ then $x \sim a$, so we have $x \sim b$ and so $x \in [b]$. Conversely, if $x \in [b]$ so $x \sim b$ then we have $x \sim a$ and so $x \in [a]$. This shows that $[a] = [b]$
3. Let $a, b \in S$. Suppose $[a] \cap [b] \neq \emptyset$. Choose $c \in [a] \cap [b]$. Since $c \in [a]$ we have $[c] = [a]$. Since $c \in [b]$ we have $[c] = [b]$. Thus $[a] = [c] = [b]$. □

30.7 Definition (Quotient)**.** When $\sim$ is an equivalence relation on S, the partition $p = \{[a] \mid a \in S\}$ is called the quotient of S by $\sim$ and is denoted by $S/\sim$. So we have

$$S/\sim = \{[a] \mid a \in S\}$$

30.8 Example. We construct $\mathbb{Z}$ from $\mathbb{N}$ using a quotient construction.

We define a relation $\sim$ on $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$ by defining $(a, b) \sim (c, d) \Leftrightarrow a + d = b + c$. We check that $\sim$ is an equivalence relation. We define

$$\mathbb{Z} = \mathbb{N}^2/\sim = \{[(a, b)] \mid a \in \mathbb{N},\, b \in \mathbb{N}\}$$

For $n \in \mathbb{N}$ we write

$$n = [(n, 0)] = \{(n, 0), (n + 1, 1), \cdots\}$$
$$-n = [(0, n)] = \{(0, n), (1, n + 1), \cdots\}$$

and we consider $\mathbb{N}$ to be a subset of Z when actually we have an injective map $\phi\colon \mathbb{N} \to \mathbb{Z}$ given by $\phi(n) = n = [(n, 0)]$.

30.9 Example. We construct $\mathbb{Q}$ from $\mathbb{Z}$ as follows. we define $\sim$ on $\mathbb{Z} \times (\mathbb{Z} \times \{0\})$ by $(a, b) \sim (c, d) \Leftrightarrow a + d = b + c$. Then $\mathbb{Q} = (\mathbb{Z} \times (\mathbb{Z} \times \{0\}))/\sim$

Lecture 31, Nov. 7

31.1 Definition (Representative)**.** For $x, a \in S$ with $\sim$m when $x \in [a]$, that is when $[x] = [a]$, we say that x is a representative of the equivalence class $[a]$.

31.2 Definition. Let $n \in \mathbb{Z}^+$. Define a relation on $\mathbb{Z}$ as follows. For $a, b \in \mathbb{Z}$, we define

$$\begin{aligned} a \sim b &\iff n \mid (a-b) \\ &\iff a - b = kn \text{ for some } k \in \mathbb{Z} \\ &\iff a = b + kn \text{ for some } k \in \mathbb{Z} \end{aligned}$$

More commonly, we write

$$a = b \mod n$$

when $a \sim b$, and we say that a is equal (or equivalent or congruent) to b modulo n.

Note that this relation is an equivalence class because for $a, b, c \in \mathbb{Z}$,

1. $a \sim a$ since $a = a + 0 \cdot n$
2. if $a \sim b$, say $a = b + k \cdot n$ with $k \in \mathbb{Z}$, then $b = a + (-k) \cdot n$, so $b \sim a$
3. if $a \sim b$, and $b \sim c$, say $a = b + kn$ and $b = c + ln$ with $k, l \in \mathbb{Z}$, then $a = c + (l + k)n$, so $a \sim c$

31.3 Definition. We define the set of integers modulo n to be the quotient set

$$\mathbb{Z}_n = \mathbb{Z}/\sim = \{[a] \mid a \in \mathbb{Z}\}$$

where

$$\begin{aligned} [a] &= \{x \in \mathbb{Z} \mid x \sim a\} \\ &= \{x \in \mathbb{Z} \mid x = a \mod n\} \\ &= \{x \in \mathbb{Z} x = a + kn \text{ for some } k \in \mathbb{Z}\} \\ &= \{\cdots, a-2n, a-n, a, a+n, a+2n, \cdots\} \end{aligned}$$

Remark. Note that for $n \in \mathbb{Z}^+$ and for $a, b \in \mathbb{Z}$, we have $a = b \mod n$ if and only if a and b have the same remainder when divided by n. That is if $a = qn + r$ with $0 \le r < n$ and $b = pn + s$ with $0 \le s < n$, then $a = b \mod n \iff r = s$

Proof. Suppose $a = qn + r$ with $0 \le r < n$ and $b = pn + s$ with $0 \le s < n$. Suppose that $a = b \mod n$, so that $n \mid (a - b)$. We have $a - b = (q - p)n + (r - s)$. Since $n \mid (a - b)$, we have $n \mid (r - s)$. If $r \neq s$ so $r - s \neq 0$ then since $n \mid (r - s)$ we have $n \le |r - s|$. But since $0 \le r < n$ and $0 \le s < n$, we have $r - s < n - s \le n - 0 = n$, and $s - r < n - r \le n - 0 = n$, so $|r - s| < n$, giving a contradiction. Thus $r = s$.

Conversely Suppose that $r = s$, then $a - b = (q - p)n + (r - s) = (q - p)n$, so $n \mid (a - b)$, hence $a = b \mod n$. □

Since the possible remainders r with $0 \le r < n$ are $0, 1, 2, \cdots, n - 1$, it follows that

$$\mathbb{Z}_n = \{[0], [1], \cdots, [n-1]\}$$

and the elements listed in the set are distinct (so that $\mathbb{Z}_n$ has exactly n elements).

Often, for $n \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$ we shall write the element $[a]$ in $\mathbb{Z}_n$ simply as $a \in \mathbb{Z}_n$. So for $a, b \in \mathbb{Z}$ we have

$$\begin{aligned} & a = b \mod n \text{ in } \mathbb{Z} \\ \iff & a = b \text{ in } \mathbb{Z}_n \end{aligned}$$

31.4 Theorem. *For $n \in \mathbb{Z}$ with $n \geq 2$, $\mathbb{Z}_n$ is a ring using the following operations: for $a, b \in \mathbb{Z}$ we define*

$$[a] + [b] = [a + b]$$

and

$$[a] \cdot [b] = [ab].$$

The zero and identity elements in $\mathbb{Z}_n$ are $[0]$ and $[1]$.

Let us verify that the operations are well-defined.

Proof. We need to show that for $a, b, c, d \in \mathbb{Z}$, if $a = c \mod n$ and $b = d \mod n$, then $a + b = c + d \mod n$ and $ab = cd \mod n$.

Let $a, b, c, d \in \mathbb{Z}$, Suppose $a = c \mod n$ and $b = d \mod n$, say $a = c + kn$ and $b = d + ln$, then $a + b = (c + d) + (l + k)n$, so $a + b = c + d \mod n$, and $ab = cd + (cl + kd + kln)n$, so $ab = cd \mod n$. □

It is easy to check that the axioms are satisfied.

For example, for $a, b, c \in \mathbb{Z}$,

$$\begin{aligned} [a] + [0] =& [a + 0] \\ =& [a] \end{aligned}$$

$$\begin{aligned} [a][1] =& [a \cdot 1] \\ =& [a] \end{aligned}$$

$$\begin{aligned} [a]([b] + [c]) =& [a][(b + c)] \\ =& [a(b + c)] \\ =& [ab + ac] \\ =& [ab] + [ac] \\ =& [a][b] + [a][c] \end{aligned}$$

31.5 Theorem (Units Modulo n)**.** *For $a, n \in \mathbb{Z}$ with $n \geq 2$.*

$$[a] \text{ is invertible in } \mathbb{Z}_n \iff gcd(a, n) = 1 \text{ in } \mathbb{Z}$$

Proof. Suppose $[a]$ is a unit in $\mathbb{Z}_n$. Choose $s \in \mathbb{Z}$ so that $[a][s] = 1$. Then $[as] = 1$ and $as = 1 \mod n$. Say $as = 1 + kn$ with $k \in \mathbb{Z}$, then $as + nt = 1$ with $t = -k$. Thus $gcd(a, n) = 1$.

Conversely, suppose $gcd(a, b) = 1$. Use the Euclidean Algorithm with Back Substitution to find $s, t \in \mathbb{Z}$ such that $as + nt = 1$.Then $as = 1 - nt$. Thus $[as] = [1]$ in $\mathbb{Z}_n$, so $[a][s] = 1$. So $[a]$ is invertible with $[a]^{-1} = [s]$ in $\mathbb{Z}_n$. □

31.6 Example. Determine whether 125 is a unit in $\mathbb{Z}_{471}$ and, if so, find 125^{-1}.

Lecture 32, Nov. 8

32.1 Example. Determine whether 125 is a unit in $\mathbb{Z}_{471}$ and, if so, find 125^{-1}.

Solution. We use EA with BS.

EA:

$$471 = 3 \cdot 125 + 96$$
$$125 = 1 \cdot 96 + 29$$
$$96 = 3 \cdot 29 + 9$$
$$29 = 3 \cdot 9 + 2$$
$$9 = 4 \cdot 2 + 1$$

BS:

$$1, -4, 13, -43, 56, -211$$

So we have $471 \cdot 56 - 125 \cdot 211 = 1$

Thus $125^{-1} = -211 = 260$ in $\mathbb{Z}_{471}$.

32.2 Definition (Group)**.** A group is a set G with an element e (called the identity element) and one binary operation $*\colon G \times G \to G$ such that

1. $*$ is associative. For all $a, b, c \in G$ we have
$$a * (b * c) = (a * b) * c$$
2. e is an identity for all $a \in G$
$$a * e = e * a = a$$
3. every $a \in G$ has a inverse. For all $a \in G$ there exists $b \in G$ such that
$$a * b = b * a = e$$

32.3 Definition (Abelian Group)**.** A group G is called abelian (or commutative) when

4 $*$ is commutative. For all $a, b \in G$ we have
$$a * b = b * a$$

Note.

1. the identity element $e \in G$ is unique. For all $a, u \in G$, if ($a * u = a$ or $u * a = a$) then $e = u$
2. the inverse of $a \in G$ is unique. For all $a, b, c \in G$, if ($a * b = e$ and $c * a = e$) then $b = c$

32.4 Example. When R is a ring, R is also an abelian group under its addition operation $+$ (which we can call the additive group of R).

32.5 Example. Also when R is a ring, the set of all invertible elements in R under multiplication is a group, which we call the group of units of R, and denoted by R^* or $R^\times$

Remark. A product of two units is a unit.

32.6 Example. When F is a field, all non zero elements in F are invertible, so $F^* = F\backslash\{0\}$

32.7 Example. $(\mathbb{Z}[\sqrt{2}])^* = \{\pm u^k \mid k \in \mathbb{Z}\}$

32.8 Definition. The group of units in $\mathbb{Z}_n$ is called the group of units modulo n and it is denoted by U_n

$$\begin{aligned} U_n = \mathbb{Z}_n^* =& \{a \in \mathbb{Z}_n \mid a \text{ is invertible } \} \\ =& \{a \in \{1, 2, 3, \cdots, n\} \mid gcd(a, n) = 1\} \end{aligned}$$

Remark. The reason we can write $gcd(a, n)$ is because $gcd(a, n) = gcd([a], n)$

Remark. For $n \in \mathbb{Z}$ with $n \geq 2$ and $a, b \in \mathbb{Z}$, we <u>cannot</u> define

$$gcd([a], [b]) = gcd(a, b)$$

because for $a, b, c, d \in \mathbb{Z}$, $a = c \mod n$ and $b = d \mod n$ do not imply that $gcd(a, b) = gcd(c, d)$.

32.9 Definition (Euler phi function)**.** The map $\varphi\colon \mathbb{Z}^+ \to \mathbb{Z}^+$ denoted by $\varphi(n) = |U_n|$ for $n \geq 2$, (where for a finite set S, $|S|$ denotes the number of elements in S), is called the Euler phi function.

So we have

$$\begin{aligned} \varphi(n) =& |U_n| = |\{a \in \mathbb{Z}_n \mid gcd(a, n) = 1\}| \\ =& \text{the number of integers } a \text{ with } 1 \leq a \leq n \text{ such that } gcd(a, n) = 1 \end{aligned}$$

32.10 Example. $\varphi(20) = 8$.

32.11 Example. When p is prime and $k \in \mathbb{Z}^+$,

$$\varphi(p^k) = p^k - p^{k-1}$$

32.12 Theorem. *For*

$$n = \prod_{i=1}^{l} p_i^{k_i}$$

where p_i are distinct primes and $k_i \in \mathbb{Z}^+$

$$\begin{aligned} \varphi(n) =& \varphi(\prod_{i=1}^{l} p_i^{k_i}) \\ =& \prod_{i=1}^{l} \varphi(p_i)^{k_i} \\ =& \prod_{i=1}^{l} p_i^{k_i}(1 - \frac{1}{p_i}) \\ =& n \prod_{i=1}^{l} (1 - \frac{1}{p_i}) \\ =& n \prod_{p|n} (1 - \frac{1}{p}) \end{aligned}$$

Powers Modulo n

32.13 Example. What day will it be in 2^{100} days?

Lecture 33, Nov. 9

Powers Modulo n

mod 5 in $\mathbb{Z}_5$

x	0	1	2	3	4
x^2	0	1	4	4	1
x^3	0	1	3	2	4
x^4	0	1	1	1	1
x^5	0	1	2	3	4

mod 7 in $\mathbb{Z}_7$

x	0	1	2	3	4	5	6
x^2	0	1	4	2	2	4	1
x^3	0	1	1	6	1	6	6
x^4	0	1	2	4	4	2	1
x^5	0	1	4	5	2	3	6
x^6	0	1	1	1	1	1	1
x^7	0	1	2	3	4	5	6

mod 20 in $\mathbb{Z}_{20}$

x	0	1	2	3	4	5
x^2	0	1	4	9	16	5
x^3	0	1	8	7	4	.
x^4	0	1	16	1	.	.
x^5	0	1	12	.	.	.
x^6	0	1	4	9	16	5

33.1 Conjecture. for $n \in \mathbb{Z}^+$ 2^{n-1} mod n $\iff$ n is prime. This is false

33.2 Theorem (Fermat's Little Theorem)**.** *let p be a prime then*

1. *for all $a \in \mathbb{Z}$ such that $gcd(a, p) = 1$,*
$$a^{p-1} = 1 \mod p$$
2. *for all $a \in \mathbb{Z}$,*
$$a^p = a \mod p$$

Proof. 1. Let p be prime. Let $a \in \mathbb{Z}$ with $gcd(a, p) = 1$. Then a i invertible in $\mathbb{Z}_p$. Define $F\colon \mathbb{Z}_p \to \mathbb{Z}_p$, by $F(x) = ax$. Note that F is bijective with inverse function $G\colon \mathbb{Z}_p \to \mathbb{Z}_p$, given by $G(x) = a^{-1}x$. Aso note that $F(0) = 0$. So F gives a bijection $F\colon U_p \to U_p$. That is $F\colon \{1, 2, 3 \cdots, p-1\} \to \{1, 2, 3 \cdots, p-1\}$. In other words,
$$\{1, 2, 3 \cdots, p-1\} = \{1 \cdot a, 2 \cdot a, \cdots, (p-1) \cdot a\}$$
Thus
$$(1 \cdot a)(2 \cdot a) \cdots ((p-1) \cdot a) = 1 \cdot 2 \cdot 3 \cdots (p-1)$$
therefore
$$a^{p-1} = 1$$
in $\mathbb{Z}_p$.

2. Let p be prime. Let $a \in \mathbb{Z}$. If $gcd(a,p) = 1$ in so $p \not| a$ then by 1, we have $a^{p-1} = 1$ in $\mathbb{Z}_p$. So we can multiply both sides by a to get

$$a^p = a$$

in $\mathbb{Z}_p$ If $gcd(a,p) \neq 1$ so $gcd(a,p) = p$ so $p \in a$, then $a = 0 \in \mathbb{Z}$ so $a^p = 0^p = 0 = a \in \mathbb{Z}_p$

□

33.3 Theorem (Euler-Fermat Theorem)**.** *Let $n \in \mathbb{Z}^+$. For all $a \in \mathbb{Z}$ with $gcd(a,n) = 1$,*

$$a^{\varphi(n)} = 1 \mod n$$

Proof. Let $n \in \mathbb{Z}^+$. When $n = 1$ we have $\varphi(n) = 1$. So for $a \in \mathbb{Z}$, $a^{\varphi n} = a^1 = a$.

Suppose $n \geq 2$. Let $a \in \mathbb{Z}$ with $gcd(a,n) = 1$. Since $gcd(a,n) = 1$, we have $a \in U_n$. The function $F\colon U_n \to U_n$ given by $F(x) = ax$ is bijective with inverse $G\colon U_n \to U_n$, given by $G(x) = a^{-1}x$. So the set U_n is equal to the set $\{ax \mid x \in U_n\}$. It follows that

$$\prod_{x \in U_n} (ax) = \prod_{x \in U_n} x$$

then

$$a^{\varphi(n)} = 1$$

in U_n. □

33.4 Theorem. *Let G be a finite commutative group. Then for all $a \in G$,*

$$a^{|G|} = 1$$

(where for a finite set S, $|S|$ denotes the number of elements in S)

Divisibility Test in Base 10

Let $n = \sum_{i=0}^{m} d_i 10^i$ where each $d_i \in \{1, 2, \cdots, 9\}$.

Noto that $2 \mid 10$, so $2^k \mid 10^k$ and $2^k \mid 10^l$ for all $l \geq k$.So

$$10^l = 0 \in \mathbb{Z}_{2^k} \text{ when } l \geq k$$

So in $\mathbb{Z}_{2^k}$,

$$n = \sum_{i=0}^{m} d_i 10^i = \sum_{i=0}^{k-1} d_i 10^i$$

So $2^k \mid n \iff 2^k$ divides the tailing k-digit number of n.

Similarly we have Divisibility Test for $3, 9, 11$.

Lecture 34, Nov. 11

34.1 Theorem (Fermat's Little Theorem)**.** *let p be a prime then*

1. *for all $a \in \mathbb{Z}$ such that $gcd(a,p) = 1$,*
$$a^{p-1} = 1 \mod p$$
2. *for all $a \in \mathbb{Z}$,*
$$a^p = a \mod p$$

34.2 Theorem (Euler-Fermat Theorem)**.** *Let $n \in \mathbb{Z}^+$. For all $a \in \mathbb{Z}$ with $gcd(a,n) = 1$,*
$$a^{\varphi(n)} = 1 \mod n$$

34.3 Example. Find 2^{-1} in $\mathbb{Z}_1 1$

Solution (Solution 1). In $\mathbb{Z}_1 1$, $2^{-1} = 6$ because $2 \cdot 6 = 12 = 1$.
Solution (Solution 2). Since $2^{10} = 1 \mod 11$ by Fermat's Little Theorem, so $2^{-1} = 2^9 = 6 \mod 11$.

34.4 Definition (Cyclic)**.** We say that a group G with $|G| = n$ is cyclic and is generated by $u \in G$ when
$$G =< u >= \{u^k \mid k \in \mathbb{Z}\}$$

Fact: When p is an odd prime, U_p^k is cyclic.
Remark.
$$U_1 1 =< 2 >=< 2^k > \text{ for all } k \in U_{10} =< 2 >=< 5 >=< 7 >=< 6 >$$

34.5 Example. Consider the Diophantine equation $x^2 + y^2 = n$ where $n \in \mathbb{N}$. Show that if $n = 3 \mod 4$ then there are no solutions.

Solution. In $\mathbb{Z}_4$,

x	0	1	2	3
x^2	0	1	0	1

For $x, y \in \mathbb{Z}_4$,
$$\begin{aligned} x^2 + y^2 \in & \{0+0, 0+1, 1+0, 1+1\} \\ = & \{0, 1, 2\} \end{aligned}$$

Solution. In $\mathbb{Z}_7$,

x	0	1	2	3	4	5	6
x^2	0	1	4	2	2	4	1
x^3	0	1	1	6	1	6	6
$3x^2$	0	3	5	6	6	5	3
$3x^2 + 4$	4	0	2	3	3	2	0

For $x, y \in \mathbb{Z}_7$, since $3x^2 + 4 = y^3$ in $\mathbb{Z}_7$,

It follows that if $3x^2 + 4 = y^3$ in $\mathbb{Z}_7$, then $x = 0, 6 \mod 7$ and $y = 0 \mod 7$.

34.6 Exercise. Try the example in $\mathbb{Z}_9$.

34.7 Example. Determine whether $2^{70} + 3^{70}$ is prime.

Solution. In $\mathbb{Z}_{13}$, powers repeat every 12, so $2^{70} + 3^{70} = 2^{10} + 3^{10} = 10 + 3 = 13$, thus $13 \mid 2^{70} + 3^{70}$

34.8 Theorem (Linear Congruence Theorem)**.** *Let $n \in \mathbb{Z}^+$, let $a, b \in \mathbb{Z}$, let $d = gcd(a, n)$. Consider the equation*

$$ax = b \mod n$$

1. *The equation $ax = b \mod n$ has a solution $x \in \mathbb{Z}$ if and only if $d \mid b$*
2. *If $x = u$ is a solution (so that $au = b \mod n$), then the general solution is*

$$x = u + k\frac{n}{d} \text{ for } k \in \mathbb{Z}.$$

Proof. This is essentially a restatement of the Linear Congruence Theorem (the LDET) because x is a solution to $ax = b \mod n \iff thereexistk \in \mathbb{Z}ax = b + kn \iff thereexisty \in \mathbb{Z}ax + ny = b$ □

Proof. 1. TFAE

   (a) The equation $ax = b \mod n$ has a solution $x \in \mathbb{Z}$
   (b) Exists $x, y \in \mathbb{Z}$ such that $ax + ny = b$
   (c) $d \mid b$ (By LDET)

2. Suppose $x = u$ is a solution so that $au = b \mod n$. Thus by the LDET, the general solution to the equation $ax + ny = b$ is
$$(x, y) = u + k\frac{n}{d}, ...$$
   Thus $u + k\frac{n}{d}$ are solutions.

□

Lecture 35, Nov. 14

35.1 Theorem (Linear Congruence Theorem)**.** *Let $n \in \mathbb{Z}^+$, let $a, b \in \mathbb{Z}$, let $d = gcd(a, n)$. Consider the equation*

$$ax = b \mod n$$

1. *The equation $ax = b \mod n$ has a solution $x \in \mathbb{Z}$ if and only if $d \mid b$*
2. *If $x = u$ is a solution (so that $au = b \mod n$), then the general solution is*

$$x = u + k\frac{n}{d} \text{ for } k \in \mathbb{Z}.$$

35.2 Theorem (Chinese Remainder Theorem)**.** *Let $n, m \in \mathbb{Z}^+$ and let $a, b \in \mathbb{Z}$. Then the pair of congruences*

$$x = a \mod n$$

$$x = b \mod m$$

has a solution $x \in \mathbb{Z}$ if and only if $d \mid (b - a)$ where $d = gcd(m, n)$, and if $x = u$ is one solution to the pair of congruences then the general solution is $x = u \mod l$ where $l = lcm(n, m)$.

Proof. Suppose the pair of congruences has a solution. Choose a solution $x \in \mathbb{Z}$ (so we have $x = a \mod n$ and $x = b \mod m$). Since $x = a \mod n$, we can choose s so that $x = a + ns$, and since $x = b \mod m$, we can choose t so that $x = b + mt$. Then $a + ns = b + mt$, so $ns - mt = b - a$. By the Linear Diophantine Equation Theorem, for $d = gcd(m, n)$, we have $d \mid (b - a)$.

Conversely, suppose that $d \mid (b - a)$. By the Linear Diophantine Equation Theorem we can choose $s, t \in \mathbb{Z}$ so that $ns - mt = b - a$. Then $a + ns = b + mt$. Let $x = a + ns$ (so $x = b + mt$). Then since $x = a + ns$ we have $x = a \mod n$. Since $x = b + mt$ we have $x = b \mod m$.

Suppose that $x = u$ is a solution to the pair of congruences. So we have $u = a \mod n$ and $u = b \mod m$. Let $k \in \mathbb{Z}$. Let $x = u + kl$ where $l = lcm(m, n)$. Since $l = lcm(m, n)$, choose $s, t \in \mathbb{Z}$ so that $l = ns = mt$. Since $x = u + kl = u + kns$, we have $x = u \mod n$ so $x = a \mod n$. Similarly we have $x = b \mod m$. Thus $x = u + kl$ is a solution to the pair of congruences.

Conversely, let x be any solution to the pair of congruences. So we have $x = a \mod n$ and $x = b \mod m$. Since $x = a \mod n$ and $u = a \mod n$, we have $x - u = 0 \mod n$, thus $n \mid x - u$. Since $x = b \mod m$ and $u = b \mod m$, we have $x = u = 0 \mod m$, so $m \mid x - u$. Since $n \mid (x - u)$ and $m \mid (x - u)$, it follows from the following lemma that $l \mid (x - u)$ since $l = lcm(m, n)$. Since $l \mid (x - u)$ we have $x = u \mod l$ as required. □

35.3 Lemma. *Let $n, m \in \mathbb{Z}^+$ and let $l = lcm(m, n)$. For every $k \in \mathbb{Z}$, if $n \mid k$ and $m \mid k$ then $l \mid k$.*

Proof. Let $k \in \mathbb{Z}^+$ with $n \mid k$ and $m \mid k$. Write $k = \prod_{i=1}^{q} p_i^{m_i}$ where $q \in \mathbb{Z}^+$, the p_i are distinct primes and each $m_i \in \mathbb{Z}^+$. Since $n \mid k$, every prime factor p of n is also a factor of k, so we can write $n = \prod_{i=1}^{q} p_i^{j_i}$ with each $j_i \in \mathbb{N}$. Similarly, we can write $m = \prod_{i=1}^{q} p_i^{k_i}$ with each $k_i \in \mathbb{N}$.

Since $n \mid k$ we have $j_i \leq m_i$ for all indices i. Since $m \mid k$, we have $k_i \leq m_i$ for all indices i. Since $m_i \geq j_i$ and $m_i \geq k_i$, we have $m_i \geq max(j_i, k_i)$. Thus

$$\prod_{i=1}^{q} p_i^{max(j_i,k_i)} \mid \prod_{i=1}^{q} p_i^{m_i}$$

that is

$$lcm(m,n) \mid k$$

□

35.4 Theorem. *For*

$$n = \prod_{i=1}^{q} p_i^{k_i}$$

where $q \in \mathbb{Z}^+$, the p_i are distinct primes, and each $k_i \in \mathbb{Z}^+$, we have

$$\varphi(n) = \prod_{i=1}^{q} \varphi(p_i^{k_i}) = \prod_{i=1}^{q} p_i^{k_i} - p_i^{k_i - 1}$$

Proof. By induction, it suffices to show that for all $l, m \in \mathbb{Z}^+$ with $gcd(l,m) = 1$, we have $\varphi(lm) = \varphi(l)\varphi(m)$. We shall prove that $|U_{lm}| = |U_l \cdot U_m|$.

Define $F\colon \mathbb{Z}_{lm} \to \mathbb{Z}_l \times \mathbb{Z}_m$ by $F(x) = (x, x)$ for $x \in \mathbb{Z}$ (that is $F(x \mod lm) = (x \mod l, x \mod m)$). Note that F is well-defined, which means that for all $x, y \in \mathbb{Z}$ if $x = y \mod lm$ then $x = y \mod k$ and $x = y \mod m$ (if $x = y \mod lm$, say $x = y + tlm$ then $x = y + (tl)m$ so $x = ymodm$)
Note that F is bijective by the (RT indeed F is surjective (onto) because given $a, b \in \mathbb{Z}$ we can solve $x = a \mod l$ and $x = b \mod m$ and then $F(x) = (x \mod l, x \mod m) = (a, b)$ and F is injective by the Chinese Remainder Theorem.

Finally, it remains to show that F restricts to a bijective map

$$F\colon U_{lm} \to U_l \times U_m$$

that is for all $x \in \mathbb{Z}$, if $gcd(x, lm) = 1$ then $gcd(x, l) = 1$ and $gcd(x, m) = 1$, and if $gcd(x, l) = 1$ and $gcd(x, m) = 1$, then $gcd(x, lm) = 1$. □

Lecture 36, Nov. 15

36.1 Example. Solve

$$\begin{aligned} 5x &= 9 \mod 14 \\ 7x &= 4 \mod 15 \end{aligned}$$

Solution. Euclidean Algorithm

$$\begin{aligned} 14 &= 2 \times 5 + 4 \\ 5 &= 1 \times 4 + 1 \\ &= 1 \times (14 - 2 \times 5) + 1 \\ 3 * 5 &= 1 \times 14 + 1 \end{aligned}$$

Let $x = 14k + 13$, then

$$\begin{aligned} 7(14k + 13) &= 4 \mod 15 \\ 8k &= 3 \mod 15 \end{aligned}$$

By inspection, $k = 2 \times 8k = 3 \mod 15$, then $k = 15t + 6$

$$\begin{aligned} x &= 14(15t + 6) + 13 \\ &= 210t + 97 \end{aligned}$$

Thus $x = 97 \mod 210$ is the solution

Cryptography

Primality Test Given an integer p, determine if p is prime.

36.2 Example (Trial Division)**.** $\forall 2 \leq d \leq \sqrt{p}$, if $\exists d \mid p$, then p is composite. Otherwise p is prime.

36.3 Definition (Algorithm Efficiency)**.** We call $f(n) \in O(g(n))$ if $\exists M, N \, \forall n > N \;\; f(n) \leq Mg(n)$.

36.4 Definition (Efficient)**.** An algorithm is efficient if its worst-case running time on n-bit input is $O(n^k)$ for some k. (Note: The original way of finding if p is prime is growing exponentially, but we want polynomial growth to be "efficient")

36.5 Example. Input: a, b n-bit integer Output:

$$\begin{aligned} a + b \\ a = (a_n + 1.....a_0)_2 \\ b = (b_n + 1.....b_0)_2 \end{aligned}$$

Each bit take at most 2 ops. In total at most 2n ops which takes O(n) time. Which means that the multiplication of the prime number of take $O(n^2)$ time.

36.6 Algorithm (Repeated Square Algorithm)**.**

$$a^k = \prod a^{2^i} \mod n$$

36.7 Example.

$$
\begin{aligned}
3^{13} \mod 19 & \\
13 &= 2^3 + 2^2 + 1 \\
3 &= 3 \mod 19 \\
3^2 &= 9 \mod 19 \\
3^4 &= 81 \mod 19 \\
&= 5 \mod 19 \\
3^8 &= 5^2 = 25 = 6 \mod 19 \\
3^{13} &= 3^8 3^4 3^1 = 14 \mod 19
\end{aligned}
$$

Lecture 37, Nov. 16

37.1 Algorithm (Fermat Test)**.** *Input n.*

Each step randomly choose $a \in [1, n-1]$ with $gcd(a, n) = 1$. If $a^{n-1} \neq 1 \mod n$ then n is composite. Otherwise repeat. After repeating $k-$times, output n is probably prime.

37.2 Definition. Let n be composite and $gcd(a, n) = 1$. We call a is a Fermat witness if $a^{n-1} \neq 1 \mod n$, otherwise we call a a Fermat Liar.

37.3 Example. 1 is always a Fermat Liar.

37.4 Proposition. *If there exists a Fermat Witness, then at least half of $a \in [1, n-1]$ ($gcd(a, n) = 1$) are Fermat Witness.*

Proof. Let $a_1, a_2, \cdots, a_r$ are all Fermat Liars. Let a be a Fermat Witness. Then we have aa_i with $i \in [1, r]$ are Fermat Witness. □

37.5 Definition (Carmichael Number)**.** A composite n is called Carmichael number if for all a with $gcd(a, n)$ we have $a^{n-1} = 1 \mod n$.

37.6 Lemma. *Let n be prime. The solution to $x^2 = 1 \mod n$ are exactly $x = \pm 1 \mod n$.*

Proof. Since $x^2 = 1 \mod n$, then $n \mid (x^2 - 1)$ and then $n \mid (x+1)(x-1)$. Since n is prime, then either $n \mid (x+1)$ or $n \mid (x-1)$. □

37.7 Proposition. *Let n be prime with $gcd(a, n) = 1$.*

$$n - 1 = 2^r d$$

then either $a^d = 1 \mod n$ or at least one of

$$a^d, a^{2d}, a^{2^2 d}, a^{2^3 d}, \cdots, 2^{2^{r-1} d} = -1 \mod n$$

37.8 Algorithm (Miller-Rabin Test)**.** *Input odd n. Then $n - 1 = 2^r d$ where d is odd. Each step randomly pick $a \in [1, n-1]$ with $gcd(a, n) = 1$.*

Compute

$$\begin{gathered} a^d \mod n \\ a^{2d} \mod n \\ a^{2^2 d} \mod n \\ \cdots \\ a^{2^{r-1} d} \mod n \end{gathered}$$

If $a^d \neq 1 \mod n$ and all the remainders above $\neq -1$, then output n is composite. After $k-$time, output n is probably prime.

37.9 Definition. Let n be composite and $gcd(a, n) = 1$. We call a a strong lair if a lies to you in Miller-Rabin test. Otherwise we call it a strong witness.

37.10 Proposition. *Let n be composite. At least $3/4$ of $a \in [1, n-1]$ with $gcd(a, n) = 1$ are strong witness.*

Lecture 38, Nov. 18

Cryptography

38.1 Example. Alice and Bob agrees on a permutation of alphabet, for example

1. $A \to Z$
2. $B \to Y$

38.2 Definition (Symmetric-Key Cryptosystem)**.**

$$\begin{aligned} M &= \text{set of messages} \\ C &= \text{set of cipher text} \\ K &= \text{set of keys} \\ E &: K \times M \to C \\ D &: K \times C \to M \\ D(K, E(K, M)) &= M \text{ where } E(K, M) = C \end{aligned}$$

38.3 Definition (Advanced Encryption System)**.** Public-key Cryptosystem

- In 1973, Ralph Markle
- In 1976, Diffie-Hellman
- In 1977, RSA public-key

38.4 Example (Merkle's puzzle)**.**

38.5 Definition (Public-Key Cryptosystem)**.**

$$\begin{aligned} &M, C \\ K_1 &= \text{set off public key} \\ K_2 &= \text{set of private key} \\ E &: K_1 \times M \to C \\ D &: K_2 \times C \to M \\ D(K_{private}, E(K_{public}, M)) &= M \text{ where } E(K_{public}, M) = C \\ &(K_{private}, K_{public}) \text{ is a valid pair} \end{aligned}$$

38.6 Algorithm (RSA Key Generation)**.** *Bob*

1. *generates two large prime* p, q
2. *Compute* $n = pq$.
3. *compute* $\phi(n) = (p-1)(q-1)$
4. *Randomly choose* $e \neq 1$, $gcd(e, \phi(n)) = 1$.
5. *Solve* $ed \equiv 1 \mod \phi(n)$.

Then Bob has Public Key (n, e), Private Key d.

Encryption: To send $m \in [0, n-1]$. Compute $c = m^e \mod n$. Send c to Bob.

Decryption: Compute $c^d \mod n = m'$

Claim. $m = m'$

Proof.

$$\begin{aligned} m' \equiv & c^d \mod n \\ \equiv & (m^e)^d \mod n \\ \equiv & m^{ed} \mod n \\ \equiv & m^{k\phi(n)+1} \mod n \\ \equiv & m \mod n \end{aligned}$$

Since $m \in [0, n-1]$, we have $m' = m$. □

38.7 Definition. We call A can be polynomial-time reduced to B, if we can solve A using polynomial time algorithm and we call the solver of B polynomially many times $A \leq B$

If $A \leq B, B \leq A$, we call A and B are polynomial-time equivalent $A \equiv B$

The adversary

P_1: Factor $n = pq$

P_2: Find $\phi(n)$

P_3: Find d

P_4: Given n, e and $m^e \mod n$, Find m. (called RSA Problem)

We have $P4 \leq P3 \leq P2 \leq P1$.
Claim. $P_2 \equiv P_1 \equiv P_3$

The security of RSA is based on the RSA Problem.

Lecture 39, Nov. 21

39.1 Definition (RAS)**.** Key Generation: Randomly pick p,q primes $n = pq$ pick $e \cdot d = 1 \mod \phi(n)$ Encryption: $c = m^e \mod \phi(n)$

Some attack on RSA Collect a lot of $n_i = p_i \cdot q_i$. Compute gcd of n_i, j_i where $i \neq j$. Some gcds are not equal to 1 and thus n_i can be factored.

$$\text{number of primes} < 2^{512} \approxeq \frac{2^{512}}{512 \cdot log2}$$
$$\text{number of primes} < 2^{511} \approxeq \frac{2^{511}}{511 \cdot log2}$$
$$\text{number of primes with 512 bits} \approxeq 2^{500}$$

39.2 Example. Sometimes e = 3

Advantage: faster encryption

Disadvantage: $n \approxeq 2^{2048}$ if $m < 2^{600} m^3 \mod n = m^3$ as integer

In practice: Padding of m is about 600, where the total from 1 random m is about 2000.

Digital Signature

1. Authentic
2. Alice which is the sender cannot deny the message she sent (non-repudiation)

39.3 Example (Naive TSA Signature)**.** (Where Alice sent a message to Bob and Eve is the outsider)

(n,e) is a public key for Alice

d is a private key for Alice

$$S = m^d \mod n$$

Bob will verify by comparing $S^e \mod n$ (where S is the signature).

Attack Models

1. Key-Only Attack: Eve only knows Alice's public key
2. Known-Message attack: Eve knows some (m_i, s_i)
3. Chosen-message attack (CMA): Eve can obtain signature s_i for arbitrary message m_i.
4. Totally broken: Eve can sign any message m.
5. Selection Forgery: Eve can sign one message of her choice.

6. Existential Forgery (ET): There exist a message that Eve can sign.

   Note. We call Digital Signature a secure if Eve cannot achieve ET using CMA.

Claim. For the pervious exmaple: (1,1) is always valid, and thus we claim that it is totally broken under CMA

Proof. Given any m, Pick $a, b \neq 1$ such that $a \cdot b = m \mod n$

Eve can obtain $s_1 = a^d \mod n$ and $s_2 = b^d \mod n$. Then $s_1 \cdot s_2 = (ab)^d = m^d \mod n$. □

To make it more secure, we will apply some functions on the message on called the hash function.

39.4 Example (Hash Function)**.** $H : \{0,1\}^k \to \{0,1\}^n$ is takes an infinite set to a finite set.

Preimage Resistant: for every y, it is hard to find H(m)= y

2nd Preimage Resistant: for every value of m, it is hard to find $m' \neq m$ such that $H(m) = H(m')$

Collision Resistant: it is hard to hard m and m' with $H(m) = H(m')$

Note: Collision Resistant implies 2nd Preimage Resistant. For such function, it should occur that $H(a, b) \neq H(a) \cdot H(b)$

39.5 Example. if H is not preimage resistant, then Eve can find m such that H(m) = 1

Since 1 is a signature for m, if H is not collision resistant, Eve can compute m, m' a collision

Under a CMA, request signature for m' that's also signature for m.

Lecture 40, Nov. 22

40.1 Example. Using RSA, Alice wants to receive a message from Bill. Alice chooses two large primes p, q, then calculate $n = pq$ and $\varphi = \varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1)$ (or $\varphi = lcm(p-1, q-1)$). Then she chooses e with $gcd(e, \varphi) = 1$. Then calculate $d = e^{-1} \mod \varphi$. Then she makes public the pair (n, e).

Bob converts this message to a number m with $m \leq n$ (or several such numbers). Bob calculates and sends $c = m^e \mod n$.

Alice receives the message by calculating $c^d \mod n$. Since the table of powers repeats every φ rows, and $ed = 1 \mod \varphi$, $c^d = (m^e)^d = m^{ed} = m^{1+k\varphi} = m \mod n$.

Here ends Chapter 4: Integers Modulo n

Chapter 5: Complex numbers

$$\mathbb{C} = \mathbb{R}^2 = \{(x, y) \mid x \in \mathbb{R}, y \in \mathbb{R}\}$$

In $\mathbb{C}$ we write

$$0 = (0, 0),\ 1 = (1, 0),\ i = (0, 1)$$

and for $x, y \in \mathbb{R}$ we write

$$x = (x, 0), iy = yi = (0, y)$$
$$x + iy = x + yi = (x, y).$$

For $z = x + iy$ with $x, y \in \mathbb{R}$, x is called the real part of z and y is called the imaginary part and we write Re(z) = x, lm(z) = y.

We define addition and multiplication in $\mathbb{C}$ by

$$(a + ib)(c + id) = (a, b) + (c, d) = (a + c, b + d) = (a + c) + i(b + d)$$

and

$$(a + ib)(c + id) = (ac - bd) + i(ad + bc)$$

40.2 Theorem. $\mathbb{C}$ *is a field.*

Proof. We only bother to show that every non-zero $z \in \mathbb{C}$ has a inverse.

Let $z = a + ib$ with $a, b \in \mathbb{R}$ and $(a, b) \neq (0, 0)$. We need to find $w = x + iy$ with $x, y \in \mathbb{R}$ such that $zw = 1$. That is

$$(a + ib)(x + iy) = 1 + 0i$$

Then

$$(ax - by) + i(ay + bx) = 1 + 0i$$

So we need

$$ax - by = 1$$
$$ay + bx = 0$$

by solving the equations we get

$$x = \frac{a}{a^2 + b^2}$$
$$y = \frac{-b}{a^2 + b^2}$$

Therefore

$$w = x + iy = \frac{a}{a^2 + b^2} + i\frac{-b}{a^2 + b^2}$$

□

40.3 Definition. For $z = x + iy$ with $x, y \in \mathbb{R}$, the conjugate of z is

$$\overline{z} = x - iy$$

and the norm (or the length) of z is

$$|z| = \sqrt{x^2 + y^2}$$

40.4 Theorem (Properties of Conjugate and Norm)**.**

1. $\overline{\overline{z}} = z$
2. $\overline{z + w} = \overline{z} + \overline{w}$
3. $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$
4. $z + \overline{z} = 2 \cdot Re(z)$
5. $z - \overline{z} = 2i \cdot Im(z)$
6. $|\overline{z}| = |z|$
7. $z \cdot \overline{z} = |z|^2$
8. *If* $z \neq 0$ *then* $|z| \neq 0$ *and* $z^{-1} = \dfrac{\overline{z}}{|z|^2}$
9. $|z| \geq 0$ *with* $|z| = 0 \Leftrightarrow z = 0$
10. $|zw| = |z|\,|w|$ *(*$|z + w| \neq |z| + |w|$*)*
11. $||z| + |w|| \leq |z + w| \leq |z| + |w|$ *(Triangle Inequality)*

40.5 Theorem. *Every non-zero complex number has exactly two complex square roots.*

Proof. Let $z = a + ib$ with $a, b \in \mathbb{R}$ and $(a, b) \neq (0, 0)$. We need to find $w = x + iy$ with $x, y \in \mathbb{R}$ such that $w^2 = z$.

We have

$$w^2 = z$$
$$(x + iy)^2 = a + ib$$
$$(x^2 - y^2) + i(2xy) = a + ib$$

then

$$x^2 - y^2 = a$$
$$2xy = b$$

by solving the equations with respect to x we get

$$x^2 = \frac{a + \sqrt{a^2 + b^2}}{2}$$

$$y^2 = x^2 - a = \frac{-a + \sqrt{a^2 + b^2}}{2}$$

Then we must have

$$w = x + iy = \pm\sqrt{\frac{a + \sqrt{a^2 + b^2}}{2}} \pm i\sqrt{\frac{-a + \sqrt{a^2 + b^2}}{2}}$$

To get $2xy = b$ we need that if $b > 0$,

$$w = x + iy = \pm\left(\sqrt{\frac{a + \sqrt{a^2 + b^2}}{2}} + i\sqrt{\frac{-a + \sqrt{a^2 + b^2}}{2}}\right)$$

and if $b < 0$, then

$$w = x + iy = \pm\left(\sqrt{\frac{a + \sqrt{a^2 + b^2}}{2}} - i\sqrt{\frac{-a + \sqrt{a^2 + b^2}}{2}}\right)$$

and when $b = 0$, then

$$w = \begin{cases} \pm\sqrt{a} & \text{if } a > 0 \\ \pm\sqrt{-a} & \text{if } a < 0 \end{cases}$$

□

40.6 Example. In $\mathbb{C}$,

$$\begin{aligned}\sqrt{3 + 4i} &= \pm\left(\sqrt{\frac{3 + \sqrt{3^2 + 4^2}}{2}} + i\sqrt{\frac{-3 + \sqrt{3^2 + 4^2}}{2}}\right) \\ &= \pm(2 + i)\end{aligned}$$

Lecture 41, Nov. 23

Note. The Quadratic Formula works in $\mathbb{C}$.

For $z, w \in \mathbb{C}$, we have $\sqrt{zw} = \sqrt{z}\sqrt{w}$, provided that $\sqrt{z}, \sqrt{w}$ denote both of the two square roots.

For $a, b, c \in \mathbb{C}$ with $a \neq 0$,

$$\begin{aligned} & az^2 + bz + c = 0 \\ \iff & z^2 + \frac{b}{a}z + \frac{c}{a} = 0 \\ \iff & (z + \frac{b}{2a})^2 = \frac{b^2 - 4ac}{4a^2} \\ \iff & z = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \end{aligned}$$

41.1 Example. Solve

$$z^2 + (2 - i)z + (2 + 2i) = 0$$

Solution.

$$\begin{aligned} z =& \frac{-(2 - i) \pm \sqrt{(2 - i)^2 - 4(2 + 2i)}}{2} \\ =& \frac{(-2 + i) \pm \sqrt{-5 - 12i}}{2} \end{aligned}$$

$$\sqrt{-5 - 12i} = \pm \left(\sqrt{\frac{-5 + \sqrt{5^2 + 12^2}}{2}} - i\sqrt{\frac{5 + \sqrt{5^2 + 12^2}}{2}} \right) = \pm(2 - 3i)$$

$$\begin{aligned} z =& \frac{(-2 + i) \pm \sqrt{-5 - 12i}}{2} \\ =& \frac{(-2 + i) \pm (2 - 3i)}{2} \\ =& -i \text{ or } -2 + 2i \end{aligned}$$

Polar Coordinates

41.2 Definition. For $0 \neq z \in \mathbb{C}$, the angle (or argument) of z is the angle $\theta = \theta(z)$ such that

$$z = |z| \cos\theta + i\,|z| \sin\theta$$

We can consider the angle θ to be the unique real number $\theta \in [0, 2\pi)$ such that $z = |z| \cos\theta + i\,|z| \sin\theta$, or we can consider the angle θ to be any real number such that $z = |z| \cos\theta + i\,|z| \sin\theta$ (in which case θ is not unique), or we can consider θ to be the set of all such real numbers

$$\begin{aligned} \theta(z) =& \{\theta \in \mathbb{R} \mid z = |z| \cos\theta + i\,|z| \sin\theta\} \\ =& \{\theta_0 + 2\pi k \mid k \in \mathbb{Z}\} \end{aligned}$$

where $\theta \in [0, 2\pi)$ with $z = |z| \cos\theta + i\,|z| \sin\theta$. In this final case, $\theta(z) = [\theta_0]$ under the equivalence relation $\sim$ on $\mathbb{R}$ defined as follows: for $\alpha, \beta \in \mathbb{R}$, $\alpha \sim \beta \iff \alpha = \beta + 2\pi k$ for some $k \in \mathbb{Z}$. Then we have

$$\theta(z) \in \mathbb{R}/\sim$$

Note. For $0 \neq z$ with $z = x + iy$ with $x, y \in \mathbb{R}$,

$$z = re^{i\theta} = r\cos\theta + ir\sin\theta$$

with $r, \theta \in \mathbb{R}$ (usually with $r > 0$).

$$\begin{gathered}
x = r\cos\theta \\
y = r\sin\theta \\
\tan\theta = y/x \text{ if } x \neq 0 \\
r^2 = x^2 + y^2 \\
r = \sqrt{x^2 + y^2} \\
\theta = \begin{cases}
\tan^{-1}(y/x) + 2\pi k, \;\; k \in \mathbb{Z} & \text{if } x > 0 \\
\cos^{-1} \frac{x}{\sqrt{x^2+y^2}} + 2\pi k, \;\; k \in \mathbb{Z} & \text{if } y > 0 \\
\tan^{-1}(y/x) + \pi k, \;\; k \in \mathbb{Z} & \text{if } x < 0 \\
2\pi k - \cos^{-1} \frac{x}{\sqrt{x^2+y^2}}, \;\; k \in \mathbb{Z} & \text{if } y < 0 \\
\sin^{-1} \frac{y}{\sqrt{x^2+y^2}} + 2\pi k &
\end{cases}
\end{gathered}$$

41.3 Example.

$$\begin{aligned}
2e^{-i\pi/6} =& 2(\cos(-\pi/6) + i\sin(-\pi/6)) \\
=& \sqrt{3} - i
\end{aligned}$$

41.4 Example.

$$e^{i\pi} = -1$$

When we write $z = x + iy$ with $x, y \in \mathbb{R}$, we have expressed z in Cartesian coordinates. When we write $z = re^{i\theta}$ with $r, \theta \in \mathbb{R}$, we have expressed z in polar coordinates.

41.5 Example. Find a formula for multiplication of complex numbers in polar coordinates.

Solution. Let $z = re^{i\alpha}$ and $w = se^{i\beta}$ where $r, s, \alpha, \beta \in \mathbb{R}$. Then

$$\begin{aligned}
zw =& re^{i\alpha} se^{i\beta} \\
=& r(\cos\alpha + i\sin\alpha)s(\cos\beta + i\sin\beta) \\
=& rs((\cos\alpha\cos\beta - \sin\alpha\sin\beta) + i(\cos\alpha\sin\beta + \sin\alpha\cos\beta)) \\
=& rs(\cos(\alpha+\beta) + i\sin(\alpha+\beta)) \\
=& rse^{i(\alpha+\beta)}
\end{aligned}$$

Thus to multiply z and w in $\mathbb{C}$, we multiply the length and add the angle.

41.6 Example. For $z = re^{i\theta}$ with $r \neq 0$,

$$z^{-1} = (re^{i\theta})^{-1} = \frac{1}{r}e^{-i\theta}$$
$$z^n = r^n e^{in\theta}$$

41.7 Definition. for $\theta \in \mathbb{R}$,

$$e^{i\theta} = \cos\theta + i\sin\theta$$
$$e^{-i\theta} = \cos\theta - i\sin\theta$$
$$\cos\theta = \frac{e^{i\theta} + e^{-i\theta}}{2}$$
$$\sin\theta = \frac{e^{i\theta} - e^{-i\theta}}{2i}$$

41.8 Definition. For $z \in \mathbb{C}$ we make the following definitions. For $z = x + iy$ with $x, y \in \mathbb{R}$,

$$e^z = e^{x+iy} = e^x e^{iy} = e^x(\cos y + i\sin y)$$

and

$$\cos z = \frac{e^{iz} + e^{-iz}}{2}$$
$$\sin z = \frac{e^{iz} - e^{-iz}}{2i}$$

Lecture 42, Oct. 25

42.1 Example.

$$\begin{aligned}(1+i)^10 =&(\sqrt{2}e^{i\pi/4})^{10}\\ =&32e^{i5\pi/2}\\ =&32e^{i\pi/2}\\ =&32i\end{aligned}$$

Note (Non-uniqueness of the Polar Representation). For $r, s, \alpha, \beta \in \mathbb{R}$ with $r, s > 0$,

$$re^{i\alpha} = se^{i\beta} \iff r = s \text{ and } \alpha = b \bmod 2\pi$$

42.2 Theorem. *Every non-zero complex number has exactly n distinct complex n-th roots for $n \in \mathbb{Z}^+$. For $z = re^{i\theta}$ with $r > 0$, the n-th roots of z are the complex numbers*

$$w = \sqrt[n]{r}e^{i(\theta+2\pi k)/n}$$

with $k \in \mathbb{Z}_n$

Proof. Let $z = re^{i\theta}$ with $r, \theta \in \mathbb{R}$ with $r > 0$. We need to solve $w^n = z$ for $w \in \mathbb{C}$. Let $w = se^{i\alpha}$ with $s, \alpha \in \mathbb{R}$, $s > 0$. Then

$$\begin{aligned}w^n = z \iff&(se^{i\alpha})^n = re^{i\theta}\\ \iff&s^n e^{in\theta} = re^{i\theta}\\ \iff&s^n = r \text{ and } n\alpha = \theta + 2\pi k \text{ for some } k \in \mathbb{Z}\\ \iff&s = \sqrt[n]{r} \text{ and } \alpha = \frac{\theta}{n} + \frac{2\pi k}{n} \text{ for some } k \in \mathbb{Z}\\ \iff&w = se^{i\alpha} = \sqrt[n]{r}e^{i(\theta+2\pi k)/n} \text{ for some } k \in \mathbb{Z}\\ \iff&w = se^{i\alpha} = \sqrt[n]{r}e^{i(\theta+2\pi k)/n} \text{ for some } k \in \mathbb{Z}_n\end{aligned}$$

□

Notation. When x is real (and non negative), $\sqrt{x} = x^{1/2}$ normally denotes the unique non-negative square root of x. When z is complex with $z \neq 0$, $\sqrt{z}$ sometimes denotes one of the two square roots, and sometimes denotes both. Similar remarks hold for n-th roots of z.

42.3 Example. Find

$$\sqrt[6]{-1+\sqrt{3}i}$$

Solution.

$$\begin{aligned}-1+\sqrt{3}i &= 2e^{i2\pi/3}\\ \sqrt[6]{-1+\sqrt{3}i} &= \sqrt[6]{2}e^{i(\pi/9+k\pi/3)} \text{ for } k \in \mathbb{Z}_6\end{aligned}$$

42.4 Example (Application)**.** Find a closed-form formula for x_n where $x_0 = 1$, $x_1 = 1$, $x_n = 2x_{n-1} - 5x_{n-2}$ for $n \geq 2$.

Solution. Let $f(z) = z^2 - 2z + 5$. The roots for $f(z)$ are

$$z = 1 \pm 2i$$

Then by the Linear Recursion Theorem, there exist $A, B \in \mathbb{C}$ such that

$$x_n = A(1+2i)^n + B(1-2i)^n$$

To get $x_0 = 1$ we have $A + B = 1$.

To get $x_1 = 1$ we have $(A+B) + 2i(A-B) = 1$.

Then $A = B = 1/2$. Therefore

$$x_n = \frac{1}{2}(1+2i)^n + \frac{1}{2}(1-2i)^n$$

Note that $1 + 2i = \sqrt{5}e^{i\theta}$ with $\theta = \tan^{-1} 2$. So

$$\begin{aligned} x_n =& \frac{1}{2}(1+2i)^n + \frac{1}{2}(1-2i)^n \\ =& \frac{1}{2}(\sqrt{5}e^{i\theta})^n + \frac{1}{2}(\sqrt{5}e^{-i\theta})^n \\ =& \frac{\sqrt{5}^n}{2}(e^{in\theta} + e^{-in\theta}) \\ =& \frac{\sqrt{5}^n}{2}(\cos(n\theta) + i\sin(n\theta) + \cos(n\theta) - i\sin(n\theta)) \\ =& \sqrt{5}^n \cos(n\theta) \end{aligned}$$

Thus

$$x_n = \sqrt{5}^n \cos(n \tan^{-1} 2)$$

42.5 Example. Find

$$\sum_{k=0}^{\infty} \binom{l}{1+3k}$$

where $\binom{m}{l} = 0$ for $l > m$.

Solution. Let $\alpha = e^{i3\pi/3}$, then $1 + \alpha + \alpha^2 = 0$.

$$\begin{aligned} (1+1)^m =& \binom{n}{0} + \binom{n}{0} + \binom{n}{0} + \binom{n}{0} + \binom{n}{0} + \cdots \\ \alpha^2(1+\alpha)^m =& \binom{n}{0}\alpha^2 + \binom{n}{0} + \binom{n}{0}\alpha + \binom{n}{0}\alpha^2 + \binom{n}{0} + \cdots \\ \alpha^2(1+\alpha^2)^m =& \binom{n}{0}\alpha + \binom{n}{0} + \binom{n}{0}\alpha^2 + \binom{n}{0}\alpha + \binom{n}{0} + \cdots \end{aligned}$$

$$\begin{aligned}3\sum_{k=0}^{\infty}\binom{l}{1+3k} =&(1+1)^m+\alpha^2(1+\alpha)^m+\alpha^2(1+\alpha^2)^m\\ =&2^m+2\cos\frac{(m-2)\pi}{3}\end{aligned}$$

Lecture 43, Nov. 28

43.1 Theorem (Fundamental Theorem of Algebra)**.** *Every non-constant polynomial with coefficients in* $\mathbb{C}$ *has a root in* $\mathbb{C}$*.*

Consequently, every non-constant $f(z) \in \mathbb{C}[z]$ *can be expressed as*

$$f(z) = c\prod_{i=1}^{n}(z - a_i)$$

where each $a_i \in \mathbb{C}$ *and* $0 \neq c \in \mathbb{C}$*. Alternatively every* $f(z)$ *of degree* n *can be expressed as*

$$f(z) = c\prod_{i=1}^{l}(z - a_i)^{k_i}$$

where $l \in \mathbb{Z}^+$*, the* a_i *are distinct complex numbers,* $k_i \in \mathbb{Z}^+$ *with* $\sum_{i=1}^{l} k_i = n$*.*

Note. Let $f(x) \in \mathbb{R}[x]$ say

$$f(x) = c_0 + c_1x + \cdots + c_nx^n, \;\; c_n \neq 0$$

If $\alpha \in \mathbb{C}$ then

$$f(\overline{\alpha}) = \overline{f(\alpha)}$$

It follows that if $f(\alpha) = 0$ then $f(\overline{\alpha}) = 0$. Consequently, every non-constant polynomial $f(x) \in \mathbb{R}[x]$ factors in $R[x]$ into a product of linear and quadratic terms.

Lecture 44, Nov. 29

44.1 Example. Let $f(x) = x^5 - 1$. For $x \in \mathbb{C}$, $f(x) = 0 \Leftrightarrow x^5 = 1$.

Then $x \in \{1, \alpha, \alpha^2, \alpha^3, \alpha^4\}$.

Then

$$\begin{aligned} f(x) =& (x-1)(x^2 - ux + 1)(x^2 - vx + 1) \\ f(x) =& (x-1) - (u+v)x^3 + (2+uv)x^2 - (u+v)x + 1 \end{aligned}$$

where $u = 2\cos(2\pi/5)$, $v = 2\cos(4\pi/5)$

Also

$$f(x) = (x-1)(x^4 + x^3 + x^2 + x + 1)$$

Comparing coefficient gives

$$\begin{aligned} u + v =& \quad -1 \\ 2 + uv =& \quad 1 \end{aligned}$$

Then we have $u = \frac{-1 \pm \sqrt{5}}{2}$. Similarly $v = \frac{-1 \pm \sqrt{5}}{2}$. Since $u = 2\cos\frac{2\pi}{5} > 0$ and $v = 2\cos\frac{4\pi}{5} < 0$, we have $u = \frac{-1+\sqrt{5}}{2}$ and $v = \frac{-1-\sqrt{5}}{2}$.

Thus

$$\cos\frac{4\pi}{5} = \frac{-1-\sqrt{5}}{4}, \ \cos\frac{2\pi}{5} = \frac{-1+\sqrt{5}}{4}$$

44.2 Example. We can solve any cubic equation

$$ax^3 + bx^2 + cx + d = 0$$

where $a, b, c, d \in \mathbb{C}$.

Step 1. Divide by a

$$x^3 + Bx^2 + Cx + D = 0$$

Step 2. Complete the cube. Change $x = y - \frac{B}{3}$.

$$0 = (y - \frac{B}{3})^3 + B(y - \frac{B}{3})^2 + C(y - \frac{B}{3}) + D = y^3 + py + q$$

for some p, q. Step 3. Let $y = z - \frac{p}{3z}$ to get

$$0 = y^3 + py + q = (z - \frac{p}{3z})^3 + p(z - \frac{p}{3z}) + q = z^3 + q - (\frac{p}{3z})^3$$

Step 4. Multiply by z^3 to get

$$z^6 + qz^3 - \frac{p^3}{37} = 0$$

Step 5. Solve for z^3 using the Quadratic Formula.

Remark. Either one of the two solutions for z^3 will produce all three solutions to $f(x) = 0$.

44.3 Example. Let $f(x) = x^3 - 3x + 1$. Solve $f(x) = 0$ for $x \in \mathbb{R}$.

Solution. Let $x = z + 1/z$. Then

$$z^3 + 1/z^3 + 1 = 0$$

Then

$$z^3 = e^{\pm i2\pi/3}$$

Then

$$z \in \{e^{i2\pi/9}, e^{i8\pi/9}, e^{i14\pi/9}\}$$

Then

$$x = 2\,\mathrm{Re}(z) \in \{2\cos(2\pi/9), 2\cos(8\pi/9), 2\cos(14\pi/9)\}$$

44.4 Definition. Let R be a commutative ring. For $a, b \in R$, we say a divides b, and we write $a \mid b$, when $b = ac$ for some $c \in R$. We say that a and b are associates, and we write $a \sim b$ when $a \mid b$ and $b \mid a$.

In an exercise, it was shown that if R is an integral domain then $a \sim b \Leftrightarrow a = bu$ for some unit $u \in R$.

For $a \in R$ we say that a is reducible when $a \neq 0$ and a is not a unit and $a = bc$ for some non-units $b, c \in R$. We say it is irreducible when $a \neq 0$ and a is not a unit and and a is not reducible.

For $a \in R$, we say that a is prime when $a \neq 0$ and a is not a unit and for all $ab \in R$, if $a \mid bc$ then either $a \mid b$ or $a \mid c$.

Lecture 45, Nov. 30

45.1 Definition. A unique factorization domain (or UFD) is an integral domain R such that

1. for every non-zero non-unit $a \in R$ we have $a = p_1 p_2 \cdots p_l$ for some $l \in \mathbb{Z}^+$ and some irreducible elements p_i and
2. the above factorization is unique up to order and association: for every non-zero non-unit $a \in R$, if $a = p_1 p_2 \cdots p_l = q_1 q_2 \cdots q_m$ with $l, m \in \mathbb{Z}^+$ and the p_i, q_j are all irreducible, then $l = m$ and there exists a bijection
$$\sigma \colon \{1, 2, \cdots l\} \to \{1, 2, \cdots l\}$$
such that $p_i \sim q_{\sigma(i)}$ for all $i \in \{1, 2, \cdots l\}$

Note. If in an integral domain R, we have a function $N \colon R \to \mathbb{N}$ such that

1. $N(a) = 0 \Leftrightarrow a = 0$
2. $N(a) = 1 \Leftrightarrow a$ is a unit.
3. for all non-zero non-unit $a, b, c \in \mathbb{R}$, if $a = bc$, then $N(b) < N(a)$ and $N(c) < N(a)$.

then (by induction) property (1) holds in the definition of a UFD.

4 for all $a, b \in R$ with $b \neq 0$ there exist $q, r \in R$ such that $a = qb + r$ and $N(r) < N(B)$.

then as in Z we can use the Euclidean Algorithm with Back-Substitution to find $d = gcd(a, b)$ and find $s, t \in R$ such that $as + bt = d$ and to show that every irreducible $a \in R$ is also prime and hence to prove that R is a UFD

Remark (Remark About Polynomials).

1. Given a polynomial $f(x) = \sum_{i=0}^{n} c_i{}^{x_i} \in R[x]$ with $c_i \in R$ with $c_n \neq 0$ so $deg(f) = n$, then we have a corresponding function $f \colon R \to R$ given by $f(x) = \sum_{i=0}^{n} c_i{}^{x_i}$.
2. If R is not commutative, then the product of polynomials is not the same as the product of their function.
3. When R is finite, equality in $R[x]$ is not the same as equality in R^R.
4. if f is an integral domain, then $deg(fg) = deg(f) + deg(g)$.q

Lecture 46, Dec. 2

46.1 Theorem (Division Algorithm)**.** *Let R be a ring, let $f, g \in R[x]$ and suppose the leading coefficient of g is a unit in R, then there exists unique $q, r \in R[x]$ such that $f = qg + r$ and $\deg r < \deg g$ (with $\deg 0 = -1$)*

Proof. First we prove existence. If $\deg f < \deg g$, then we can take $q = 0$ and $r = f$. Suppose $\deg f \geq \deg g$, say

$$f(x) = \sum_{i=0}^{n} a_i{}^{x_i}$$

$a_i \in R$, $a_n \geq 0$, and

$$g(x) = \sum_{i=0}^{m} b_i{}^{x_i}$$

$b_i \in R$ and b_m is a unit in R, then $n = \deg f \geq \deg g = m$, so $n - m \geq 0$. The polynomial

$$a_n {b_m}^{-1} x^{n-m} g(x)$$

has degree n with leading coefficient a_n (the same as f), so

$$f(x) - a_n {b_m}^{-1} x^{n-m} g(x)$$

has degree less than n.

By a suitable induction hypothesis, we can suppose that

$$f(x) - a_n {b_m}^{-1} x^{n-m} g(x) = p(x)g(x) + r(x)$$

where $p, r \in R[x]$ with $\deg r < \deg g$. Then we have

$$f(x) = q(x)g(x) + r(x)$$

with $q(x) = a_n {b_m}^{-1} x^{n-m} + p(x)$.

Next we prove uniqueness. Suppose $f = qg + r = pg + s$, where $q, r, p, s \in R[x]$ with $\deg s, \deg r < \deg g$. Then $(q - p)g = s - r$. If $p - q \neq 0$ then $\deg(p - q) \geq 0$, so $\deg((q - p)g) = \deg(q - p) + \deg g \geq \deg g$. But $\deg(s - r) < \deg g$. So we must have $q - p = 0$. It follows that $s = r$. □

Consequences

46.2 Theorem (The Remainder Theorem)**.** *Let R be a commutative ring. Let $f \in R[x]$ and let $a \in R$. Then when we divide $f(x)$ by $(x - a)$. Then the remainder is a constant polynomial $r(x) = r \in R$ and $r = f(a)$.*

Proof. Write

$$f(x) = q(x)(x - a) + r$$

Then

$$f(a) = r$$

□

46.3 Theorem (The Factor Theorem)**.** *Let R be an integral domain. Let $f \in R[x]$ and let $a \in R$. The a is a root of f if and only if $(x - a) \mid f(x)$.*

Proof. Suppose $f(a) = 0$. Write $f(x) = q(x)(x-a)+r$. Then $r = 0$. So $f(x) = q(x)(x-a)$. So $(x-a) \mid f(x)$.

Conversely, if $(x - a) \mid f(x)$, we can choose $q(x) \in R[x]$ so that $f(x) = q(x)(x - a)$, then $f(a) = 0$. □

46.4 Theorem. *Let R be an integral domain and let $0 \neq f \in R[x]$, with $\deg f = n$. Then f has at most n roots.*

Proof. When $\deg f = 0$, f is a non-zero constant polynomial, so f has no roots. Let $n = \deg f > 0$. Suppose that $a \in R$ is a root of f, so $f(a) = 0$. Then $(x - a) \mid f(x)$, say

$$f(x) = (x - a)g(x)$$

Then $\deg g = n - 1$. So we can suppose inductively, that g has at most $n - 1$ roots. we need to show that every root b of f with $b \neq a$ is also a root of g. Let $b \in R$ be a root of f with $b \neq a$. Since $f(x) = (x-a)g(x)$, $0 == f(b) = (b - a)g(b)$. Since $(b - a)g(b) = 0$ and $b - a \neq 0$, then $g(b) = 0$, because R is an integral domain. □

46.5 Theorem. *Let F be a field and let $f \in F[x]$ be a polynomial with $\deg f = 2$ or 3. Then f is irreducible if and only if f has not roots.*

Lecture 47, Dec. 5

47.1 Definition (Content of $f \in \mathbb{Z}[x]$)**.**

47.2 Lemma (Gauss's Lemma)**.**

1. *For $f, g \in \mathbb{Z}[x]$, we have $c(fg) = c(f)c(g)$*

47.3 Theorem (Rational Roots)**.**

47.4 Theorem (Modular Reduction)**.**

47.5 Theorem (Eisenstein's criterion)**.**