Chapter 1: Numbers, Sets, and Functions

Quadratic Formula Origin

Try to solve equations $x+y=s$, $xy=p$.

We write $y=s-x$ and substitute to get $x(s-x)=p \Rightarrow x^2-sx+p=0$. Multiply by a nonzero "a" to get $ax^2-asx+ap=0$ and substitute $b=-as$ and $c=ap$ to obtain $ax^2+bx+c=0$

$$0=a\left(x^2+\frac{b}{a}x\right)+c=a\left(x^2+\frac{b}{a}x+\frac{b^2}{4a^2}\right)-\frac{b^2}{4a}+c=a\left(x+\frac{b}{2a}\right)^2+c-\frac{b^2}{4a}$$

$$\Rightarrow \left(x+\frac{b}{2a}\right)^2=\frac{b^2-4ac}{4a^2} \Rightarrow x=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$$

- ↳ when $b^2-4ac>0$ there are two values
- ↳ when $b^2-4ac=0$ there is one value (two equal values)
- ↳ when $b^2-4ac<0$ there is no real number solution

converting back to the original variables, we get

$$x=\frac{s\pm\sqrt{s^2-4p}}{2}$$

- ↳ Two values when $s^2-4p\geq 0$
- ↳ No real solution when $s^2-4p<0$

In these calculations, we used algebraic properties

Elementary Inequalities

(Assuming positive real numbers have positive square roots and the square of every real number is nonnegative)

Proposition 1.1: If $0<a<b$ then $a^2<ab<b^2$ and $0<\sqrt{a}<\sqrt{b}$

Proof: Multiply $a<b$ by a to get $a^2<ab$ and by b to get $ab<b^2$ so $a^2<ab<b^2$.
Assuming $\sqrt{b}\leq\sqrt{a}$, we get $b\leq a$ which contradicts our assumption. ☒

Definition: The **absolute value** of a real number x written $|x|$ is defined by

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

- ↳ Think of $|x|$ as the distance from x to 0
- ↳ Note: $x\leq|x|$ and $|xy|=|x||y|$

Proposition 1.3 (Triangle Inequality): If x and y are real numbers, then $|x+y|\leq|x|+|y|$

Proof: start with $2xy\leq 2|x||y|$. Adding x^2+y^2 to both sides and using $z^2=|z|^2$, we get

$$x^2+2xy+y^2\leq x^2+2|x||y|+y^2=|x|^2+2|x||y|+|y|^2$$

Using Proposition 1.1, we take the positive square root of both sides to get

$$x^2+2xy+y^2=(x+y)^2\leq|x|^2+2|x||y|+|y|^2=(|x|+|y|)^2 \Rightarrow |x+y|\leq|x|+|y| \text{ as needed } ☒$$

Definitions:

- ↳ The **arithmetic mean** (or **average**) of x and y is $\frac{x+y}{2}$
- ↳ The **geometric mean** of nonnegative numbers x and y is $\sqrt{xy}$
- ↳ The **AGM Inequality** stands for Arithmetic Mean-Geometric Mean Inequality and states that the arithmetic mean of two nonnegative numbers is at least their geometric mean

Proposition 1.4 (AGM Inequality): If x and y are real numbers then $2xy \le x^2+y^2$ and $xy \le \left(\frac{x+y}{2}\right)^2$.

If x and y are also nonnegative, then $\sqrt{xy} \le \frac{x+y}{2}$. Equality holds for both when $x=y$.

Proof: Begin with $0 \le (x-y)^2 = x^2-2xy+y^2$. Adding $2xy$ yields $4xy \le x^2+2xy+y^2 = (x+y)^2$. Dividing by 4 gives $xy \le \left(\frac{x+y}{2}\right)^2$. If $x \ge 0$ and $y \ge 0$, then $xy \ge 0$ and we take the positive square roots to get $xy \le \left(\frac{x+y}{2}\right)^2$ and $\sqrt{xy} \le \frac{x+y}{2}$ by Proposition 1.1. ▨

Corollary 1.5: If $x,y>0$ then $\frac{2xy}{x+y} \le \sqrt{xy} \le \frac{x+y}{2}$. Equality holds in each when $x=y$.

Proof: Proposition 1.4 yields $\sqrt{xy} \le \frac{x+y}{2}$. We get the other inequality by multiplying by $\frac{2\sqrt{xy}}{x+y}$.

$$\sqrt{xy}\,\frac{2\sqrt{xy}}{x+y} \le \frac{x+y}{2}\,\frac{2\sqrt{xy}}{x+y} \Rightarrow \frac{2xy}{x+y} \le \sqrt{xy}$$ ▨

Definition: The harmonic mean of x and y is $\frac{2xy}{x+y}$.

↳ This is from the study of average rates. If we travel distance d at rate r in time t we have $d=rt$. If we travel distance d at rate r_1 and time t_1 and return with rate r_2 and time t_2, then $r_1t_1 = r_2t_2 = d$. To get the average rate r of the trip, we solve $2d = r(t_1+t_2)$

$$r = \frac{2d}{t_1+t_2} = \frac{2d}{d/r_1 + d/r_2} = \frac{2r_1r_2}{r_1+r_2} = \text{harmonic mean}$$

Example: If the rate one way on a plane is 380mph and the return rate is 420mph then the average rate is: $\frac{2(380)(420)}{380+420} = \frac{800(19)(21)}{800} = 399$ mph

Sets

Definition: The notion of a set is so fundamental that we dont give a precise definition. Think of a set as a collection of distinct objects with a precise description allowing us to determine whether a given object is in it.

Definition: The objects in a set are its elements or members. When x is an element of A we write $x \in A$ and say "x belongs to A". When not in A we write $x \notin A$.

Definition: If every element of A belongs to B then A is a subset of B and B contains A. We write $A \subseteq B$ or $B \supseteq A$.

To list elements explicitly, use brackets. i.e. $A=\{-1,1\}$ is a set of elements -1 and 1. Order of elements doesnt change the set. $x,y \in S$ means both x and y are in S.

Definitions/Notation:

↳ $\mathbb{N}$ = natural numbers $= \{1,2,3,\ldots\}$

↳ $\mathbb{Z}$ = integers $= \{\ldots,-2,-1,0,1,2,\ldots\}$

↳ $\mathbb{Q}$ = rational numbers i.e. numbers that can be written a/b with $a,b \in \mathbb{Z}$, $b \neq 0$

↳ $\mathbb{R}$ = real numbers

↳ Note: $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$

Definition: Sets A and B are **equal**, i.e. $A=B$, if they have the same elements.

Definition: The **empty set**, written $\emptyset$, is the unique set with no elements

Definition: A **proper subset** of a set A is a subset of A that is not A itself.

Definition: The **power set** of a set A is the set of all subsets of A

Note: The empty set is a subset of every set.

Example: Let S be the set {Kansas, Kentucky} and let T be the set of states in the U.S. that begin with "K". S=T and S has 4 subsets: $\emptyset$, {Kansas}, {Kentucky}, {Kansas, Kentucky}. These 4 elements are the elements of the power set.

In order to specify a set consisting of elements in a set A satisfying a given condition, we write $\{x \in A: \text{condition}(x)\}$ and read "the set of x in A such that x satisfies 'condition' "

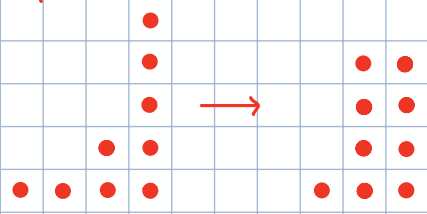
To prove that a set T is the set of solutions to a problem, we must prove that every solution belongs to T and that every member of T is a solution.

Example: Let $S=\{x \in \mathbb{R}: x^2<x\}$ and $T=\{x \in \mathbb{R}: 0<x<1\}$ and prove S=T. Let $x \in T$ then $x>0$. Multiply $x<1$ by x to get $x^2<x$ so $x \in S$. Let $x \in S$. Since $x^2<x$ we get $0>x^2-x=x(x-1)$ which means x and x-1 are nonzero with opposite signs so $x \in T$ as needed.

The Penny Problem

We are given a collection of pennies grouped into piles. We create a new pile by taking one penny from each existing pile. We consider different orderings of the same list of sizes to be equivalent. i.e. 1,3,5 = 3,1,5. We let S be the set of lists that do not change.

Example:



Let a be a list with n piles and b be the resulting new list. If $a \in S$, then a=b and b has n piles. Since we introduce one new pile to b, one pile of a must disappear, meaning a has exactly one pile of size 1. Since a=b, b has exactly one pile of size 1 too. This means a must have exactly one pile of size two. Letting i be the size of a pile we continue this reasoning for i from 1 to n-1.
If a has one pile of size i then b does too. So a has a pile of size i+1, giving us one pile of each size from 1 to n.
Let T be the set of lists consisting of one pile of each size from 1 through a natural number n. we have already shown that $S \subseteq T$ so now we need to show that all elements of T remain unchanged (i.e. $T \subseteq S$).
Consider an element of T with piles of size 1,2,...,n. For each i from 2 to n, the pile of size i becomes i-1. The pile of size 1 disappears and the n piles contribute one coin to make a pile of size n. Thus the resulting piles are the same as the original and $T \subseteq S$. So S=T.

Definitions/Notation:
↳ when $a, b \in \mathbb{Z}$ and $a \leq b$, then $\{a, \ldots, b\}$ denotes $\{i \in \mathbb{Z} : a \leq i \leq b\}$
↳ when $n \in \mathbb{N}$, then $[n]$ means $\{1, \ldots, n\}$
↳ $\{2k : k \in \mathbb{Z}\}$ is the set of even numbers
↳ $\{2k+1 : k \in \mathbb{Z}\}$ is the set of odd numbers.
↳ 0 is an even number. Every integer is either even or odd

Definition: The parity of an integer states whether it is even or odd.
↳ "Even" and "odd" is only for discussing integers. If we say a number is positive without specifying the system, we mean a positive real number.

Definition: when $a, b \in \mathbb{R}$ with $a \leq b$, the closed interval $[a, b]$ is the set $\{x \in \mathbb{R} : a \leq x \leq b\}$

Definition: When $a, b \in \mathbb{R}$ with $a \leq b$, the open interval (a, b) is the set $\{x \in \mathbb{R} : a < x < b\}$

Definition: Consider $S \subseteq \mathbb{R}$. If an element x belonging to S is at least as large as every element of S, then x is the maximum of S.
↳ Minimum is defined analogously.
↳ The open interval (a,b) has no max nor min

Definition: A list with entries in A consists of elements of A in a specified order with repetition allowed.

Definition: A k-tuple is a list with k entries.
↳ we write A^k for the set of k-tuples with entries in A.

Definition: An ordered pair is a list with two entries.

Definition: The cartesian product of sets S and T, written $S \times T$, is the set $\{(x, y) : x \in S, y \in T\}$

↳ $A^2 = A \times A$ and $A^k = \{(x_1, \ldots, x_k) : x_i \in A\}$
↳ x_i is read "x sub i"
↳ since (a,b) is used for ordered pairs, often it is written "the interval (a,b)" for open intervals

Definition: When $S = T = \mathbb{R}$, $S \times T$ or $\mathbb{R}^2$ is the set of all points in the plane designated by horizontal and vertical coordinates called the cartesian coordinates of the point.

The concept of cartesian products is named after René Descartes (1596-1650)

Definition: Let A and B be sets. Their union, written $A \cup B$, consists of all elements in A or B.

Definition: Let A and B be sets. Their intersection, written $A \cap B$, consists of all elements in both A and B.

Definition: Let A and B be sets. Their difference, $A - B$, consists of elements of A that are not in B

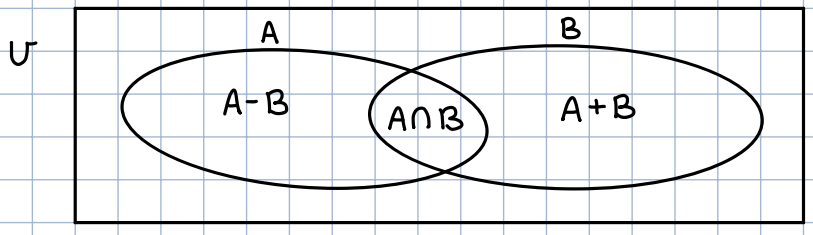
Definition: Two sets are disjoint if their intersection is $\emptyset$

Definition: If a set A is contained in some universe U, then the complement, A^c, of A is the set of elements of U not in A.

Example: Let E and O denote the sets of even numbers and odd numbers. $E \cap O = \emptyset$ and $E \cup O = \mathbb{Z}$. Within $\mathbb{Z}$, $E^c = O$.

Venn Diagram

In a venn diagram, an outer box represents the universe under consideration and the regions within the box correspond to sets. Non-overlapping regions correspond to disjoint sets.



The venn diagram was named for John Venn (1834-1923) though he didnt invent them.

Functions

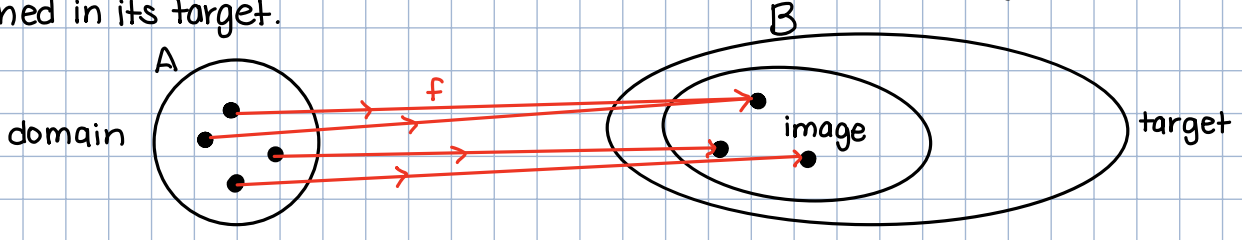
Definition: A function, f, from a set A to a set B assigns to each $a \in A$, a single element f(a) in B.

Definition: For a function f from A to B (written $f: A \to B$), the set A is the domain.

Definition: The element f(a) in set B is called the image of a under f. The image of f with domain a is $\{f(a): a \in A\}$.

Definition: For $f: A \to B$, the set B is the target.

A function $f: A \to B$ is defined on A and maps A into B. The image of a function is contained in its target.



Ways to describe a function

↳ list pairs (a, f(a))
↳ provide a formula for f(a) from a
↳ describe the rule in words

Definition: A function $f: A \to B$ is well-defined if the rules defining f assign to each element of A exactly one element of B.

Definition: A function f is real-valued if its image is a subset of $\mathbb{R}$
↳ For real-valued functions f and g, $(f+g)(x) = f(x)+g(x)$ and $(fg)(x) = f(x)g(x)$

Definition: A (real) **polynomial** in one variable is a function $f:\mathbb{R}\to\mathbb{R}$ defined by $f(x)=c_0+c_1x^1+\ldots+c_kx^k$ where k is a non-negative integer and $c_0,\ldots,c_k$ are real numbers.

Definition: For real polynomial $f(x)=c_0+c_1x^1+\ldots+c_kx^k$. $c_0,\ldots,c_k$ are called the **coefficients** of f

Definition: For real polynomial $f(x)=c_0+c_1x^1+\ldots+c_kx^k$, the **degree** of f is the largest d such that $c_d\neq 0$

↳ The polynomial with all coefficients 0 has no degree.

Polynomial Names / Definitions

↳ Degree 0 = constant

↳ Degree 1 = linear

↳ Degree 2 = quadratic

↳ Degree 3 = cubic

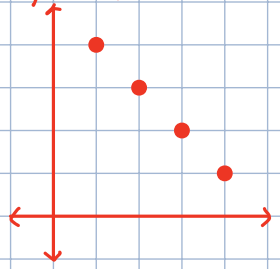
Definition: A **monomial** in variables $x_1,\ldots,x_n$ is an expression $cx_1^{a_1}\cdots x_n^{a_n}$, where c is a real number and each a_j is a non-negative integer.

↳ A polynomial in n variable is a finite sum of monomials in n variables

Example: The function $f(x,y,z)=x^2+y^2+z^2+2xy+2xz+2yz$ is a polynomial in three variables.

Definition: The **graph** of a function $f:A\to B$ is the subset of $A\times B$ consisting of the ordered pairs $\{(x,f(x)):x\in A\}$

Example: we define $f:[4]\to[4]$ by $f(n)=5-n$. The graph of f is $\{(1,4),(2,3),(3,2),(4,1)\}$



Definition: A set $S\subseteq\mathbb{R}$ is **bounded** if there exists $M\in\mathbb{R}$ such that $|x|\leq M$ for all $x\in S$

Definition: A set $S\subseteq\mathbb{R}$ is **unbounded** if no such $M\in\mathbb{R}$ exists such that $|x|\leq M$ for all $x\in S$.

Definition: A **bounded function** is a real-valued function whose image is bounded. That is, for a real-valued function, f, for which there is some $M\in\mathbb{R}$ such that $|f(x)|\leq M$ for all x in the domain.

Definition: Let $f:\mathbb{R}\to\mathbb{R}$ and A be a set of real numbers. We say f is **increasing** on A if $f(x)<f(x')$ whenever $x<x'$ and $x,x'\in A$.

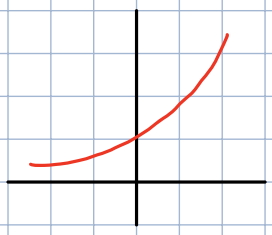
↳ Also called strictly increasing

Definition: Let $f:\mathbb{R}\to\mathbb{R}$ and A be a set of real numbers. f is **nondecreasing** on A if $f(x)\leq f(x')$ whenever $x<x'$ and $x,x'\in A$.

↳ Also called weakly increasing

Changing $<$ to $>$ and $\leq$ to $\geq$ yields definitions for decreasing and non-increasing

Definition: A function is **monotone** on A if it is non-decreasing on A or non-increasing on A.



unbounded, increasing

bounded, not monotone

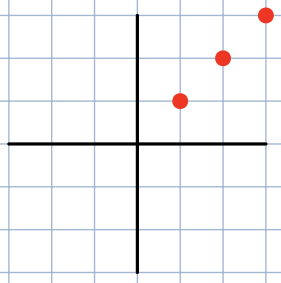
bounded, increasing

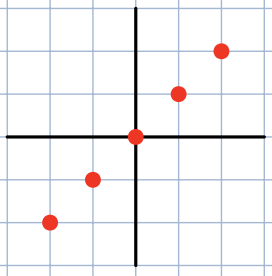
Definition: The **identity function** on a set S is the function $F: S \to S$ defined $f(x)=x$ for all $x \in S$.

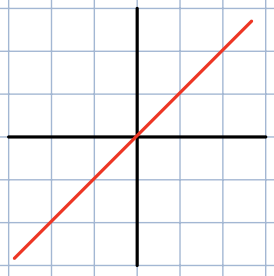
Definition: A **fixed point** of a function $f: S \to S$ is an element $x \in S$ such that $f(x)=x$

↳ Every element in the identity function is a fixed point.

↳ A function from $\mathbb{R}$ to $\mathbb{R}$ has a fixed point if and only if the line $\{(x,x)\}$ intersects its graph.







Definition: Given $f: A \to B$ and $y \in B$, the **inverse image** of y under f, written $I_f(y)$, is the set $\{x \in A : f(x)=y\}$

Definition: For $h: \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, the **level set** of h with value c is $I_h(c)$

Example: Let $A(x,y)=x+y$. For each c, $I_A(c)$ is a line in $\mathbb{R}^2$. The level sets are parallel lines whose union is $\mathbb{R}^2$.

The Real Number System

Definition: **Axioms** are a short list of properties that real numbers satisfy and from which all other properties are derived.

Definition: A set S with operations + and · and distinguished elements 0 and 1 with $0 \neq 1$ is a **field** if the following field axioms hold.

Field Axioms

A0: $x+y \in S$	← closure →	M0: $x \cdot y \in S$
A1: $(x+y)+z = x+(y+z)$	← associativity →	M1: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
A2: $x+y = y+z$	← commutativity →	M2: $x \cdot y = y \cdot z$
A3: $x+0 = x$	← identity →	M3: $x \cdot 1 = x$
A4: given x, there is a $w \in S$ such that $x+w=0$		M4: for $x \neq 0$, there is a $w \in S$ such that $x \cdot w = 1$
DL: $x \cdot (y+z) = x \cdot y + x \cdot z$ ← distributive law		↖ inverse ↗

↳ + is addition, · is multiplication, 0 is the **additive identity element**, 1 is the **multiplicative identity element**

Definition: The additive inverse of x is the negative of x, written $-x$

Definition: Subtraction of y from x is defined by $x-y = x+(-y)$

Definition: The multiplicative inverse of x is the reciprocal of x, written x^{-1}
↳ 0 has no reciprocal

Definition: Division of x by y when $y \neq 0$ is defined $\frac{x}{y} = x \cdot (y^{-1})$

↳ we write $x \cdot y$ as xy and $x \cdot x$ as x^2

Definition: A positive set in a field F is a set $P \subseteq F$ such that for $x, y \in F$ we have:

P1: $x, y \in P$ implies $x+y \in P$	closure under addition
P2: $x, y \in P$ implies $xy \in P$	closure under multiplication
P3: $x \in F$ implies exactly one of $x=0, x \in P, -x \in P$	trichotomy

Definition: An ordered field is a field with a positive set P.
↳ In an ordered field, $x<y$ means $y-x \in P$.
↳ $\leq$, $>$, and $\geq$ have analogous definitions

Definition: If $S \subseteq F$, then $\beta \in F$ is an upper bound for S if $x \leq \beta$ for all $x \in S$.

Definition: An ordered field F is complete if every non-empty subset of F that has an upper bound in F has a least upper bound in F.

Proposition 1.42: Each of $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ is closed under addition and multiplication. $\mathbb{Z}$ and $\mathbb{Q}$ are closed under subtraction. The set of non-zero numbers in $\mathbb{Q}$ is closed under division.

Proposition 1.43: Let F be an ordered field and $x, y, z, u, v \in F$.

a) $x+z=y+z$ implies $x=y$
b) $x \cdot 0 = 0$
c) $(-x)y = -(xy)$
d) $-x = (-1)x$
e) $(-x)(-y) = xy$
f) $xz = yz$ and $z \neq 0$ implies $x=y$
g) $xy=0$ implies $x=0$ or $y=0$

Proposition 1.44: Let F be an ordered field and $x, y, z, u, v \in F$.

O1: $x \leq x$	Reflexive property
O2: $x \leq y$ and $y \leq x$ imply $x=y$	Antisymmetric Property
O3: $x \leq y$ and $y \leq z$ imply $x \leq z$	Transitive Property
O4: at least one of $x \leq y$ and $y \leq x$ holds	Total ordering Property

Proposition 1.45: Let F be an ordered field and $x, y, z, u, v \in F$

F1: $x \leq y$ implies $x+z \leq y+z$	Additive Order Law
F2: $x \leq y$ and $0 \leq z$ imply $xz \leq yz$	Multiplicative Order Law
F3: $x \leq y$ and $u \leq v$ imply $x+u \leq y+v$	Addition of Inequalities
F4: $0 \leq x \leq y$ and $0 \leq u \leq v$ imply $xu \leq yv$	Multiplication of Inequalities

Proposition 1.46: Let F be an ordered field and $x, y, z, u, v \in F$

a) $x \leq y$ implies $-y \leq -x$
b) $x \leq y$ and $z \leq 0$ implies $yz \leq xz$
c) $0 \leq x$ and $0 \leq y$ imply $0 \leq xy$
d) $0 \leq x^2$
e) $0 < 1$
f) $0 < x$ implies $0 < x^{-1}$
g) $0 < x < y$ implies $0 < y^{-1} < x^{-1}$

Example: Multiply 598 by 602

$598(602) = (600-2)(600+2) = 600^2 - 2^2 = 360000 - 4 = 359996$

Example: Find all a,b for set $\{(a,b) \in \mathbb{Z}^2 : a^2b > 2a\}$

$a^2b > 2a \Rightarrow a(ab-2) > 0$

Both factors must have the same sign so either

1) $a > 0$ and $ab > 2$ ↓

all integer pairs in first quadrant except $(1,2)$ and $(2,1)$

OR

2) $a < 0$ and $ab < 2$ ↓

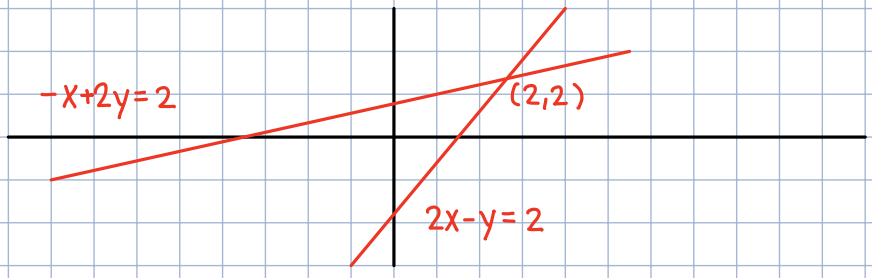
all integer pairs in second quadrant and $(-1,1)$

Thus the answer is the union of these.

Chapter 2: Language and Proofs

Definition: A linear equation in two variables x and y is an equation $ax+by=r$ where the coefficient a, b and the constant r are real numbers.

Definition: A line in $\mathbb{R}^2$ is the set of pairs (x,y) satisfying a linear equation whose coefficient a and b are not both zero.



There are three possibilities for two lines:
1) They intersect at one point → one common solution
2) They are parallel → no common solutions
3) They are identical → infinitely many solutions

Theorem 2.2: Let $ax+by=r$ and $cx+dy=s$ be linear equations in two variables x and y. If $ad-bc\neq 0$, then there is a unique common solution. If $ad-bc=0$, then there is no common solution or there are infinitely many depending on R and S.

Proof: If all four coefficients are zero, then there is no solution unless $r=s=0$ in which all (x,y) are solutions. Otherwise, at least one coefficient is non-zero. we may assume $d\neq 0$ by interchanging the equations.

Solving for y in the second equation, we get

$$y=\frac{s-cx}{d}$$

we substitute this to get

$$\left(a-\frac{bc}{d}\right)x+\frac{bs}{d}=r \quad \text{since} \quad ax+b\left(\frac{s-cx}{d}\right)=ax+\frac{bs-bcx}{d}=ax+\frac{bs}{d}-\frac{bcx}{d}=\left(a-\frac{bc}{d}\right)x+\frac{bs}{d}=r$$

multiplying by d, we get $(ad-bc)x+bs=rd$.

when $ad-bc\neq 0$, we divide to get

$$x=\frac{rd-bs}{ad-bc}$$

which we substitute back in to get

$$a\left(\frac{rd-bs}{ad-bc}\right)+by=r \Rightarrow y=\frac{r(ad-bc)-a(rd-bs)}{b(ad-bc)}=\frac{as-rc}{ad-bc} \leftarrow \text{unique solution}$$

when $ad-bc=0$, it becomes $bs=rd$. If $bs\neq rd$ then no solution. If $bs=rd$, then there are infinitely many solutions of $(x,y)=\left(x,\frac{s-cx}{d}\right)$ ☒

Theorem 2.3: If a,b,c are odd integers, then $ax^2+bx+c=0$ has no solution in the set of rational numbers.

Proof (by contradiction): Suppose x is a rational p/q for integers p and q, where x is in lowest terms so p and q have no common integer factor larger than 1.
From $ax^2+bx+c=0$, we get $ap^2+bpq+cq^2=0$.
Now, we prove $ap^2+bpq+cq^2$ cannot be 0.
Since x is a rational number in lowest terms, p and q cannot both be even. If they're both odd, then all three terms are odd so $\neq 0$.
If p is odd and q is even (or vice versa), then there are two even terms and one odd so $\neq 0$. Thus x cannot be rational. ☒

Quantifiers / Logic Statements

To understand a statement/subject it must be written about clearly.

Example: The negation of "All students are male" is not "all students are not male" but "at least one student is not male"

Math must avoid ambiguities.

Example: The sentence "There is a real number y such that $x=y^3$ for every real number x" says that some number y is the cube root of all numbers, which is false. To say that every number has a cube root, we say "for every real number x, there is a real number y such that $x=y^3$"

Definition: A mathematical statement is an unambiguous, grammatically correct sentence which can be said to be "true" or "false".

Example: Consider the statement "This statement is false" and call it P. If the words "this statement" refer to another sentence Q, then P is either true or false. However, if "this statement" refers to P itself, P must be false if it is true and true if it is false. P cannot be a mathematical statement.

Definitions/Notations:
1) We use uppercase letters to denote mathematical statements
2) The truth or falsity of a statement is its truth value.
   ↳ Negating a statement reverses its truth value
3) We use $\neg$ to indicate negation
   ↳ Example: $\neg P$ means "not P". If P is false, $\neg P$ is true.
4) In the statement "For all x in S, $P(x)$ is true", the variable x is universally quantified. We write this as $(\forall x \in S)\, P(x)$
5) $\forall$ is a universal quantifier
   ↳ meaning "for all" or "every"
6) In the statement "There exists an x in S such that $P(x)$ is true", the variable x is existentially quantified. We write this as $(\exists x \in S) P(x)$
7) $\exists$ is an existential quantifier
8) The set of allowed values for a variable is its universe.

Universal ($\forall$)	helpers	Existential ($\exists$)	helpers
for all, for every		for some	
if	then	there exists	such that
whenever, for, given every,	satisfies	at least one	for which
any, a, arbitrary	must, is	some	satisfies
let	be	has a	such that

Example: Consider the statement "If n is even, the n is the sum of two odd numbers". Letting E be the set of even integers and O be the set of odd, and letting $P(n,x,y)$ be "$n=x+y$". The statement becomes: $(\forall n \in E)(\exists x,y \in O)\, P(n,x,y)$

Example: Consider the exercise "Let a and b be real numbers. Prove that $ax^2+bx=a$ has a real solution". This becomes $(\forall a,b \in \mathbb{R})(\exists x \in \mathbb{R})(ax^2+bx=a)$. When $a=0 \Rightarrow x=0$ works for all b. When $a \neq 0$, then the quadratic formula $x=\frac{-b+\sqrt{b^2+4a^2}}{2a}$ works.

Example: Compare $(\forall x \in A)(\exists y \in B)P(x,y)$ and $(\exists y \in B)(\forall x \in A)P(x,y)$
The second statement always implies the first. The first is true if for each x we can pick a y that works. The second is true if there is a y that will always work regardless of the choice of x.

$\neg[(\forall x)P(x)]$ is the same as $(\exists x)(\neg P(x))$
$\neg[(\exists x)P(x)]$ is the same as $(\forall x)(\neg P(x))$

Example: we can use notation for unbounded and bounded
↳ bounded: $(\exists M \in \mathbb{R})(\forall x \in \mathbb{R})(|f(x)| \leq M)$
↳ unbounded: $(\forall M \in \mathbb{R})(\exists x \in \mathbb{R})(|f(x)| > M)$

Compound Statements

we can use connectives "and", "or", "if and only if", and "implies" to build compound statements

Name	Symbol	Meaning	condition for truth
Negation	$\neg P$	not P	P false
Conjunction	$P \wedge Q$	P and Q	both true
Disjunction	$P \vee Q$	P or Q	at least one true
Biconditional	$P \Leftrightarrow Q$	P if and only if Q	same truth value
Conditional	$P \Rightarrow Q$	P implies Q	Q true whenever P true

Definition: In the conditional statement $P \Rightarrow Q$, P is the hypothesis

Definition: In the conditional statement $P \Rightarrow Q$, Q is the conclusion

Definition: The statement $Q \Rightarrow P$ is the converse of $P \Rightarrow Q$

Definition: A listing of the truth value computation for each choice of truth values is a truth table

P	Q	P => Q	¬P	(¬P) ∨ Q	(P => Q) <=> ((¬P) ∨ Q)
T	T	T	F	T	T
T	F	F	F	F	T
F	T	T	T	T	T
F	F	T	T	T	T

Definition: An expression is called a tautology if its always true

A statement depending on two variables x,y needs both variables to be quantified. order matters.

Definition: Two logical expressions X,Y are logically equivalent if they have the same truth value for each assignment of truth values of the variables

Two logically equivalent statements are interchangable in a proof.

Example: For statements P,Q, the following are equivalent:

a) $\neg(P \wedge Q)$	$(\neg P) \vee (\neg Q)$
b) $\neg(P \vee Q)$	$(\neg P) \vee (\neg Q)$
c) $\neg(P \Rightarrow Q)$	$P \wedge (\neg Q)$
d) $P \Leftrightarrow Q$	$(P \Rightarrow Q) \wedge (Q \Rightarrow P)$
e) $P \vee Q$	$(\neg P) \Rightarrow Q$
f) $P \Rightarrow Q$	$(\neg Q) \Rightarrow (\neg P)$

If P(x) and Q(x) are statements about element $x \in U$, we often write $(\forall x \in U)(P(x) \Rightarrow Q(x))$ as $P(x) \Rightarrow Q(x)$ or $P \Rightarrow Q$

If $A = \{x \in U : P(x) \text{ is true}\}$ then $P(x) \Rightarrow Q(x)$ is $(\forall x \in A) Q(x)$
If $B = \{x \in U : Q(x) \text{ is true}\}$ then $P(x) \Rightarrow Q(x)$ is $A \subseteq B$ and $Q(x) \Rightarrow P(x)$ is $B \subseteq A$ and $P \Leftrightarrow Q$ is $A = B$

$x \in A^c$	<=>	not $(x \in A)$	<=>	$\neg(x \in A)$
$x \in A \cup B$	<=>	$(x \in A)$ or $(x \in B)$	<=>	$(x \in A) \vee (x \in B)$
$x \in A \cap B$	<=>	$(x \in A)$ and $(x \in B)$	<=>	$(x \in A) \wedge (x \in B)$
$A \subseteq B$	<=>	$(\forall x \in A)(x \in B)$	<=>	$(x \in A) \Rightarrow (x \in B)$

Definition: The intersection of a collection of sets consists of all elements that belong to all of the sets.

Definition: The union of a collection of sets consists of all elements that belong to at least one of the sets.

when x and y are numbers, then $x = y$ is the same as $x \leq y$ and $y \leq x$. when A and B are sets $A = B$ is the same as $A \subseteq B$ and $B \subseteq A$. For logical statements P and Q, $P \Leftrightarrow Q$ means $P \Rightarrow Q$ and $Q \Rightarrow P$

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

Elementary Proofs

Methods of proving $P \Rightarrow Q$

↳ **Direct Method**: Assume P is true and use mathematical reasoning to prove Q true

↳ **Contrapositive Method**: Prove $\neg Q \Rightarrow \neg P$

↳ **Method of contradiction**: Assume P and $\neg Q$ and obtain a contradiction

Example: If x and y are both odd integers, then $x+y$ is even.

Proof: suppose x and y are odd, then there exists integers k, ℓ such that $x = 2k+1$ and $y = 2\ell+1$. By properties of addition and the distributive law:

$$x+y = 2k+1+2\ell+1 = 2k+2\ell+2 = 2(k+\ell+1)$$

This is twice an integer so it is even.

Example: An integer is even if and only if its square is even.

If n is even, then $n = 2k$ for a $k \in \mathbb{Z}$.

$n^2 = (2k)^2 = 4k^2 = 2(2k^2)$ so the forward direction is true.

To prove the reverse, we prove that if n^2 is even, so is n. We can prove this via the contrapositive method.

Let m be an odd integer with $m = 2k+1$ for a $k \in \mathbb{Z}$.

$$m^2 = (2k+1)^2 = 4k^2+2k+1 = 2(2k+k)+1 \quad \boxtimes$$

Example: There is no largest real number.

Assume that for all $x \in \mathbb{R}$, $\exists z \in \mathbb{R}$ such that $z \geq x$. If $x = z+1$ then $z \geq z+1 \Rightarrow 0 \geq 1$ which is a contradiction. $\boxtimes$

Chapter 3: Induction

Definition: The set $\mathbb{N}$ of **natural numbers** is the intersection of all sets $S \subseteq \mathbb{R}$ that have the following two properties:

a) $1 \in S$

b) if $x \in S$, then $x+1 \in S$

Theorem 3.6 (Principle of Induction): For each natural number n, let $P(n)$ be a mathematical statement. If properties (a) and (b) hold, then for each $n \in \mathbb{N}$ the statement $P(n)$ is true.

a) $P(1)$ is true

b) For $k \in \mathbb{N}$, if $P(k)$ is true, then $P(k+1)$ is true

Proposition 3.7: For $n \in \mathbb{N}$, $1+2+\ldots+n = \frac{n(n+1)}{2}$

Proof: Since $1 = 1 \cdot 2/2$ $P(1)$ is true. Assume $P(k)$, then

$$P(k+1) = P(k) + k+1 = \frac{k(k+1)}{2} + (k+1) = (k+1)\left(\frac{k}{2}+1\right) = \frac{(k+1)(k+2)}{2}$$

Thus $P(n)$ holds. ☒

Definition: A **sequence** is a function whose domain is $\mathbb{N}$

Σ indicates summation $\quad \sum_{i=a}^{b} f(i) =$ sum of $f(i)$ over integers i where $a \le i \le b$

Proposition 3.12: Suppose $\langle a \rangle$ and $\langle b \rangle$ are sequences of real numbers and that $n \in \mathbb{N}$

a) If $c \in \mathbb{R}$, then $\sum_{i=1}^{n} c a_i = c \sum_{i=1}^{n} a_i$

b) If $a_i \le b_i$ for all $i \in \mathbb{N}$, then $\sum_{i=1}^{n} a_i \le \sum_{i=1}^{n} b_i$

c) If $0 \le a_i \le b_i$ for all $i \in \mathbb{N}$, then $\prod_{i=1}^{n} a_i \le \prod_{i=1}^{n} b_i$

where Π indicates multiplication products

Lemma 3.13: If $x, y \in \mathbb{R}$ and $n \in \mathbb{N}$, then $x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + \ldots + xy^{n-2} + y^{n-1})$

Corollary 3.14 (The Geometric Sum): If $q \in \mathbb{R}$, $q \neq 1$ and n is a non-negative integer, then

$$\sum_{i=0}^{n-1} q^i = \frac{q^n - 1}{q-1}$$

Proof: we use Lemma 3.13 with $x = q$ and $y = 1$ to get

$$q^n - 1 = (q-1)(q^{n-1} + q^{n-2} + \ldots + 1)$$

and divide by $q-1$. ☒

Example: The NCAA basketball tournament starts with 64 teams. How many games are played to get a champion?

Game Numbers: $32 \to 16 \to 8 \to 4 \to 2 \to 1$

Total games: $1+2+4+8+16+32 = \sum_{i=0}^{5} 2^i = 2^6 - 1 = 63$

Proposition 3.16: If $n \in \mathbb{N}$ and $q \geq 2$, then $n < q^n$.

Proof: Use induction.

For $n=1$, $1<q$ by definition of q.

Assume claim holds for n, then $n < q^n$. $n+1 \leq n+n = 2n \leq qk < q \cdot q = q^{k+1}$. ▨

Proposition 3.19: If $x_1, \ldots, x_n$ are numbers in the interval $[0,1]$

$$\prod_{i=1}^{n} (1-x_i) \geq 1 - \sum_{i=1}^{n} x_i$$

Proof: By induction. ▨

Corollary 3.20: If $0 \leq a \leq 1$ and $n \in \mathbb{N}$, then $(1-a)^n \geq 1-na$.

Proof: This is proposition 3.19 with $x_1 = \ldots = x_n = a$. ▨

Proposition 3.21: For all $n \in \mathbb{N}$, $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$

Proof: By induction. ▨

Lemma 3.23: If f is a polynomial of degree d, then a is a zero of f if and only if $f(x) = (x-a)h(x)$ for some polynomial h of degree $d-1$.

Proof: By definition of a polynomial, $f(x) = \sum_{i=0}^{d} c_i x^i$ with d a non-negative integer and $c_d \neq 0$. If $f(x) = (x-a)h(x)$ holds, then $f(a) = 0$.

Assuming $f(a) = 0$, then since $f(x) = c_0 + \sum_{i=1}^{d} c_i x^i$, we have

$$f(x) = f(x) - f(a) = c_0 - c_0 + \sum_{i=1}^{d} c_i (x^i - a^i) = \sum_{i=1}^{d} c_i (x^i - a^i)$$

and by Lemma 3.13 for $i \geq 1$, $x^i - a^i = (x-a)h_i(x)$, where $h_i(x) = \sum_{j=1}^{i} x^{i-j} a^{j-1}$

Using Proposition 3.12a, factoring $(x-a)$ gives $f(x) = (x-a)h(x)$, where $h(x) = \sum_{i=1}^{d} h_i(x)$.

Since each h_i has degree $i-1$, h is of degree $d-1$. ▨

Theorem 3.24: Every polynomial of degree d has at most d zeros.

Proof: Use induction with basis step $d=0$ and inductive step $d \geq 1$ ▨

Corollary 3.25: Two real polynomials are equal if and only if their corresponding coefficients are equal.

Proof: Let $f(x) = g(x)$ and $h = f - g$, then $h(x) = 0$ and by Theorem 3.24, it must be the zero polynomial since it has 0 zeroes. ▨

Strong Induction

Theorem 3.28 (Strong Induction Principle): Let $\{P(n) : n \in \mathbb{N}\}$ be a sequence of mathematical statements. If properties (a) and (b) below hold, then for every $n \in \mathbb{N}$, $P(n)$ is true.

a) $P(1)$ is true

b) For $k \geq 2$, if $P(i)$ is true for all $i < k$, then $P(k)$ is true.

Proposition 3.30 (well ordering Property): Every non-empty subset of $\mathbb{N}$ has a least element.

Theorem 3.31: $\sqrt{2}$ is irrational

Proof: If $\sqrt{2}$ is rational, then $\sqrt{2} = m/n$ for some $m, n \in \mathbb{N}$.
Since $1 < \sqrt{2} < 2$, $n < m < 2n$ so $0 < m-n < n$.
Using $2n^2 = m^2$,

$$\frac{2n-m}{m-n} = \frac{n(2n-m)}{n(m-n)} = \frac{2n^2-mn}{n(m-n)} = \frac{m^2-mn}{n(m-n)} = \frac{m(m-n)}{n(m-n)} = \frac{m}{n}$$

which is smaller than m/n but m/n was assumed to be simplified. ☒

Definition: The **Method of Descent** proves $P(n)$ for all $n \in \mathbb{N}$ by proving that there is no least n where $P(n)$ fails.

Proposition 3.32: Every natural number n can be expressed in exactly one way as the product of an odd number and a power of 2.

Proof: If the claim fails then some least n does not have a unique such expression. If n is odd, then $1 \cdot n$ is a unique such expression. If n is even then we look at $n/2$. We add a power of 2 to $n/2$ expression to produce an n. So if n is a counter example, then $n/2$ is also a counter example. ☒

Chapter 6: Divisibility

Definition: If $a, b \in \mathbb{Z}$ with $b \neq 0$, and $a = mb$ for some integer m, then a is **divisible** by b, and b divides a (written $b|a$)

Definition: when $b|a$, we call b a **divisor** or factor of a.

Definition: A natural number, other than 1, is prime if its only positive factors are itself and 1
↳ 0 and 1 are not prime.

Factors/Factorization

Definition: Integers a and b are **relatively prime** when they have no common factor greater than 1.

Definition: When m and n are integers, the number $ma+nb$ is an **integer combination** of a and b.

Lemma 6.5: If a and b are relatively prime, then there exists integers m and n such that $ma+nb=1$.

Proof: When $|a|=|b|$ or $b=0$, the numbers are not relatively prime unless $|a|=1$, in which $(m,n)=(a,0)$. We may then assume $|a|>|b|$.
Multiplying by -1 does not change common factors, so we may assume a and b are non-negative. We now use strong induction we proved the base case of $a+b=1$.
For the induction step, suppose $a+b \geq 2$. By symmetry, we may assume $a>b$.
When $b>0$, we apply the induction hypothesis to b and $a-b$. They are relatively prime and positive with sum less than $a+b$.
We obtain integers m' and n' where $m'b+n'(a-b)=1$, which is $n'a+(m'-n')b=1$.
Setting $m=n'$ and $n=m'-n'$ yields the desired combination. ☒

Proposition 6.6: If a and b are relatively prime and a divides qb, then a divides q.

Proof: Since a, b are relatively prime, Lemma 6.5, provides integers m, n such that $1=ma+nb$. Thus $q=maq+nbq=mqa+mqb$.
Since q divides each term on the right, it divides q. ☒

Proposition 6.7: If a prime p divides a product of k integers, then p divides at least one of the factors.

Proof: Induction on k.
When $k=1$, trivial. For $k \geq 2$, let $b_1, \ldots, b_k$ be k integers whose product is divisible by p and $n = \prod_{i=1}^{k-1} b_i$. Thus p divides nb_k.

If p divides b_k then the claim holds. Otherwise, since p is prime, p and b_k are relatively prime, so by Proposition 6.6, p divides n. ☒

Definition: A **prime factorization** of n expresses n as a product of powers of distinct primes, written as $n = \prod_{i=1}^{k} p_i^{e_i}$

Definition: In a prime factorization, the exponent of each prime is its multiplicity.

Example: The prime factorization of $1200 = 2^4 3^1 5^2$.

Theorem 6.9 (Fundamental Theorem of Arithmetic): Every positive integer n has a prime factorization, which is unique except for reorderings of the factors.

Corollary 6.10: If a,b are relatively prime and both divide n then $ab|n$.

Definition: Given integers a,b (not both 0), the greatest common divisor, $\gcd(a,b)$, is the largest natural number that divides both a and b.
↳ By convention, $\gcd(0,0)=0$
↳ If $d=\gcd(a,b)\neq 0$, then a/d and b/d are relatively prime.

Theorem 6.12: The set of integer combinations of a and b is the set of multiples of $\gcd(a,b)$.
Proof: Let $d=\gcd(a,b)$ and $S=\{ra+sb : r,s\in\mathbb{Z}\}$ be the set of integer combinations of a and b. Let T denote the set of multiples of d.
$S\subseteq T$:
Since d divides both a and b, there are integers k and ℓ such that $a=kd$ and $b=\ell d$.
Then, $ma+nb=mkd+n\ell d=(mk+n\ell)d$
so d divides $ma+nb$.
$T\subseteq S$:
We express each d as an integer combination of a and b.
Since a/d and b/d are relatively prime, then by Lemma 6.5 there exists integers m,n such that $m(a/d)+n(b/d)=1$. Thus $ma+nb=d$ and for $k\in\mathbb{Z}$, $(mk)a+(nk)b=kd$. ☒

Euclidean Algorithm

Definition: An algorithm is a procedure for performing a computation or construction.

Proposition 6.13: If a,b,k are integers, then $\gcd(a,b)=\gcd(a-kb,b)$.
Proof: By the distributive law, every integer dividing a and b must also divide $a-kb$. Similarly, every integer dividing $a-kb$ and b must also divide a. Thus d is a common divisor of $a-kb$ and b. Hence $\gcd(a,b)=\gcd(a-kb,b)$. ☒

Proposition 6.14: If a and b are integers with $b\neq 0$, then there is a unique integer pair k,r such that $a=kb+r$ and $0\leq r\leq |b|-1$.
↳ The process of obtaining k and r is the Division Algorithm.
↳ The resulting r is the remainder of a under division by b.
↳ r is 0 if and only if a is divisible by b.

The Euclidean Algorithm
Input: A pair of non-negative integers, both not 0
Output: The greatest common divisor of the input pair
Initialization: Set the current pair as the input pair
Iteration: If one element of the current pair is 0, then report the other element as the output and stop. Otherwise, replace the maximum element of the current pair with its remainder upon division by the other element and repeat using this pair as the current pair.

Example: Find gcd(154,35)

(154,35) $154-4(35)=14$

(35,14) $35-2(14)=7$

(14,7) $14-2(7)=0$

(7,0)

Thus 7 is the gcd and $7=35-2(14)=35-2(154-4(35))=-2(154)+9(35)$ which is the integer combination of the original inputs.

Theorem 6.17: Applied to integers (a,b) with $a \geq b \geq 0$ and $a \neq 0$, the Euclidean Algorithm reports $\gcd(a,b)$ as the output. Furthermore, reversing the substitution steps of the algorithm yields an expression of $\gcd(a,b)$ as $ma+nb$ for some $m,n \in \mathbb{Z}$

Example: The equation $6x+15y=79$ has no solution in integers as such a solution would express 79 as an integer combination of 6 and 15, but all such combinations are multiples of $\gcd(6,15)=3$ which 79 is not.

Example: what are the integer solutions of $6x+15y=99$?

99 is a multiple of $\gcd(6,15)=3$ so Theorem 6.12 guarantees a solution.

First reduce the equation to $2x+5y=33$.

Setting $x=-2$ and $y=1$, we get $2(-2)+5(1)=1$, which we multiply to get $(x,y)=33(-2,1)=(-66,33)$

Since 2,5 are relatively prime, $S=\{(-66+5k, 33-2k): k \in \mathbb{Z}\}$

Definition: An equation for which we seek integer solutions is called a diphantine equation.

Dartboard Problem

Theorem (Dartboard Problem): For a,b relatively prime, $a,b \geq 2$

1) $ab-a-b$ cannot be written as an integer combination $ax+by$
2) If $N > ab-a-b$ then $N=ax+by$ for some x,y with $xy \geq 0$

Theorem 6.21: When a,b are relatively prime and $x \in \mathbb{Z}$, the numbers $x, x+b, \ldots, x+(a-1)b$ have distinct remainders upon division by a.

Proof: Suppose $x+ib$ and $x+jb$ have the same remainder, which means $x+ib=ka+r$ and $x+jb=\ell a+r$ for some integers k,ℓ,r with $0 \leq r \leq a-1$.

Subtracting the equations gives $(i-j)b=(k-\ell)a$.

Since a divides $(k-\ell)a$, it must divide $(i-j)b$. Since a and b are relatively prime, a must divide $i-j$ and since i and j are non-negative integers less than a, $i=j$. ☒

Chapter 7: Modular Arithmetic

Relations

Definition: When S and T are sets, a relation between S and T is a subset of the product $S \times T$. A relation on S is a subset of $S \times S$.

Example: Let S be the set of students and T be the set of teachers. We define a relation R between S and T by letting R be the set of ordered pairs (x,y) in $S \times T$ such that x has taken a class from y.

Example: If $f: \mathbb{R} \to \mathbb{R}$, then the graph of f is a relation on $\mathbb{R}$. It is the set of ordered pairs $\{(x,y) \in \mathbb{R}^2 : y = f(x)\}$

Definition: An equivalence relation on a set S is a relation R on S such that for all choices of distinct $x, y, z \in S$

a) $(x,x) \in R$ — Reflexive Property
b) $(x,y) \in R \Rightarrow (y,x) \in R$ — Symmetric Property
c) $(x,y) \in R$ and $(y,z) \in R \Rightarrow (x,z) \in R$ — Transitive Property

Example: The divisibility relation $R = \{(m,n) \in \mathbb{N}^2 : m \mid n\}$ is reflexive, transitive, but not symmetric. Thus it is not an equivalence relation.

Definition: Given an equivalence relation on S, the set of elements equivalent to $x \in S$ is the equivalence class.

Congruence

Definition: Given a natural number n, the integers x and y are congruent modulo n if $x - y$ is divisible by n. We write this as $x \equiv y \pmod{n}$

Definition: For $x \equiv y \pmod{n}$, the number n is called the modulus.

Theorem 7.16: For every $n \in \mathbb{N}$, congruence modulo n is an equivalence relation on $\mathbb{Z}$.

Proof: Reflexive: $x - x = 0$ is divisible by n

Symmetric: If $x \equiv y \pmod{n}$ then $n \mid (x-y)$. since $y - x = -(x-y)$ and $n \mid (n-m)$ if and only if $n \mid m$, then $y \equiv x \pmod{n}$.

Transitive: If $n \mid (x-y)$ and $n \mid (y-z)$ then $x - y = an$ and $y - z = bn$ for some integers a, b. Adding these equations gives $x - z = an + bn = (a+b)n$ so $n \mid (x-z)$. ▨

Definition: The equivalence classes of the relation "congruence modulo n" on $\mathbb{Z}$ are the remainder classes or congruence classes modulo n. The set of congruence classes is written as $\mathbb{Z}_n$ or $\mathbb{Z}/n\mathbb{Z}$.

Lemma 7.19: If $a \equiv r \pmod{n}$ and $b \equiv s \pmod{n}$ then $a + b \equiv (r+s) \pmod{n}$ and $a \cdot b \equiv (r \cdot s) \pmod{n}$

Proof: Since $a \equiv r \pmod{n}$ and $b \equiv s \pmod{n}$ then $a = kn + r$ and $b = \ell n + s$ for som integers k, ℓ. Adding these equations yields $a + b = (k+\ell)n + (r+s)$ and thus $a + b \equiv (r+s) \pmod{n}$
Multiplying these gives $a \cdot b = k\ell n^2 + (ks + \ell r)n + rs$ and thus $a \cdot b \equiv r \cdot s \pmod{n}$ ▨

Example: Since $79 \equiv 4 \pmod 5$ and $23 \equiv 3 \pmod 5$, $79 \cdot 23 \equiv 12 \pmod 5$. Since $12 \equiv 2 \pmod 5$, we can reduce this to $79 \cdot 23 \equiv 2 \pmod 5$.

Definition: A binary operation on a set S is a function from $S \times S$ to S.
↳ On $\mathbb{Z}_n$, addition is the binary operation defined by letting the sum of the congruence classes $\bar{a}$ and $\bar{b}$ be the class containing the integer $a+b$.
↳ On $\mathbb{Z}_n$, multiplication is the binary operation defined by letting the product of $\bar{a}$ and $\bar{b}$ be the class containing the inner $a \cdot b$
↳ In notation, $\bar{a} + \bar{b} = \overline{a+b}$ and $\bar{a} \cdot \bar{b} = \overline{ab}$

Example: For $\mathbb{Z}_2$

+	0	1
0	0	1
1	1	0

•	0	1
0	0	0
1	0	1

Example: $79 \cdot 23 \equiv 4 \cdot 3 \equiv 12 \equiv 2 \pmod 5$

Lemma 7.27: If a and n are relatively prime integers, then multiplication by a defines a bijection from $\mathbb{Z}_n - \{0\}$ to itself; Equivalently, multiplication by a permutes the non-zero congruence classes.
Proof: Since a and n are relatively prime, $0, a, 2a, \ldots, (n-1)a$ all have different remainders modulo n. Since 0 has remainder 0, the others are non-zero. Since they are distinct, the list defines an injection from $\mathbb{Z}_n - \{0\}$ to itself. Since the set is finite, the injection is a bijection. ☒

Definition: A function $f: A \to B$ is a bijection if for every $b \in B$, there is exactly one $x \in A$ such that $f(x) = b$.

Definition: A function $f: A \to B$ is injective if for each $b \in B$, there is at most one $x \in A$ such that $f(x) = b$.

Corollary 7.28: If a and n are relatively prime integers, then solutions to $ax \equiv 1 \pmod n$ exists and lie in a single congruence class.
↳ In the language of $\mathbb{Z}_n$, the class $\bar{x}$ is the multiplicative inverse of a.

Applications

Theorem 7.30 (Chinese Remainder Theorem): If $\{n_i\}$ is a set of r natural numbers that are pairwise relatively prime, and $\{a_i\}$ are any r integers then the system of congruences $x \equiv a_i \pmod{n_i}$ has a unique solution $N = \pi n_i$.

Example: Suppose we seek x such that $x \equiv 2 \pmod 5$, $x \equiv 4 \pmod 7$, and $x \equiv 3 \pmod 9$. This yields $N = 315$ and $N_1, N_2, N_3 = 63, 45, 35$.

i	a_i	n_i	N_i	$N_i \pmod{n_i}$	y_i
1	2	5	63	3	2
2	4	7	45	3	5
3	3	9	35	-1	-1

By the Chinese Remainder Theorem, we get $2 \cdot 63 \cdot 2 + 4 \cdot 45 \cdot 5 + 3 \cdot 35 \cdot (-1) = 1047$. All numbers congruent to $1047 \pmod{315}$ are solutions, the smallest being $102 = 1047 - 3 \cdot 315$.

when p is prime and a is not a multiple of p then $a^{p-1} \equiv 1 \pmod{p}$

Functional Digraph

we form loops for a by calculating ax

Example: For a=5 and p=13

For x=0

For x=1

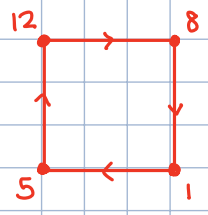
$1 \equiv 1 \pmod{13}$

$1 \cdot 5 \equiv 5 \pmod{13}$

$5 \cdot 5 = 25 \equiv 12 \pmod{13}$

$12 \cdot 5 = 60 \equiv 8 \pmod{13}$

$8 \cdot 5 = 40 \equiv 1 \pmod{13}$



For x=2

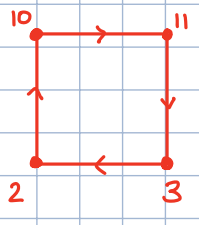
$2 \equiv 2 \pmod{13}$

$2 \cdot 5 = 10 \pmod{13}$

$10 \cdot 5 = 50 \equiv 11 \pmod{13}$

$11 \cdot 5 = 55 \equiv 3 \pmod{13}$

$3 \cdot 5 = 15 \equiv 2 \pmod{13}$



For x=4

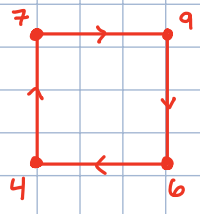
$4 \equiv 4 \pmod{13}$

$4 \cdot 5 = 20 \equiv 7 \pmod{13}$

$7 \cdot 5 = 35 \equiv 9 \pmod{13}$

$9 \cdot 5 = 45 \equiv 6 \pmod{13}$

$6 \cdot 5 = 30 \equiv 4 \pmod{13}$



Definition: When some power of a is congruent to $1 \pmod{p}$, the order of a (in $\mathbb{Z}_p$) is the least k such that $a^k \equiv 1 \pmod{p}$

Lemma 7.34: Let p be prime and suppose $a \not\equiv 0 \pmod{p}$. For $x \in \mathbb{Z}_p$, let $S_x = \{x, xa, xa^2, \ldots\}$. There is a positive integer k such that for all $x \neq 0$, the set S_x consists of exactly k elements.

Lemma 7.35: If R is the relation on $\mathbb{Z}_p$ defined by $(x,y) \in R$ if and only if $y \equiv xa \pmod{p}$ for some non-negative integer j, then R is an equivalence relation.

Proof: Since $x \equiv xa^0 \pmod{p}$, R is reflexive.

Let k be the order of a in $\mathbb{Z}_p$. When $y \equiv xa^j \pmod{p}$, we may assume $0 \leq j \leq k-1$. If $y \equiv xa^j \pmod{p}$ then $x \equiv ya^{k-j} \pmod{p}$ so symmetric. If $y \equiv xa^r \pmod{p}$ and $z \equiv xa^s \pmod{p}$, then $z = xa^{r+s} \pmod{p}$ so transitive. ☒

Theorem 7.36 (Fermat's Little Theorem): If p is prime and a is not a multiple of p, then $a^{p-1} \equiv 1 \pmod{p}$

Example: $11^{902} = 11^{30 \cdot 30 + 2} = (11^{30})^{30} \cdot 11^2 \equiv 1^{30} \cdot 121 \equiv -3 \equiv 28 \pmod{31}$

Corollary 7.39: If p is prime and $a \in \mathbb{Z}$ then $a^p \equiv a \pmod{p}$

Definition: A group is a set G together with a binary operation $\circ$ on G satisfying the following properties:

1) There is an element $e \in G$ such that for every $x \in G$, $x \circ e = x = e \circ x$. This element is the identity element.
2) For every $x \in G$, there is an element $y \in G$ such that $x \circ y = e = y \circ x$. Y is the inverse of x.
3) For every $x, y, z \in G$, $(x \circ y) \circ z = x \circ (y \circ z)$

Corollary 7.42: When p is prime, $\mathbb{Z}_p - \{0\}$ is a group under multiplication.

Lemma 7.43: If p is prime and $a \in \mathbb{N}$, then $a^2 \equiv 1 \pmod{p}$ if and only if $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$

Proof: If $a^2 \equiv 1$, then p divides $a^2 - 1 = (a+1)(a-1)$.
When a prime divides a product, it must divide one of the factors so p divides $a+1$ or $a-1$ ▨

Theorem 7.44 (Wilson's Theorem): $(p-1)! \equiv -1 \pmod{p}$ for p prime.

Chapter 8: The Rational Numbers

Recall: When p and q are integers and $q \neq 0$, the quotient p/q is a real number. Such real numbers are called rational. The others are irrational.

Rational Numbers/Geometry

Definition: A **fraction** is an expression consisting of an integer, a division symbol, and a non-zero integer. For integers a, b, we write the fraction

$$\frac{a}{b} \text{ or } a/b \qquad \frac{a}{b} \longrightarrow \text{numerator}, \quad \frac{a}{b} \longrightarrow \text{denominator}$$

Fractions a/b and c/d represent the same rational number if $ad = bc$.

Definition: A fraction a/b is in **lowest terms** if a and b have no common factors and $b > 0$

↳ when the denominator is the smallest positive number among the denominators of all representatives of the same rational number.

Proposition 8.11: Every line L in $\mathbb{R}^2$ that contains the origin and has rational slope is specified by an integer pair (a, b) (with $a \neq 0$) such that $(x, y) \in L$ if and only if $(x, y) = (at, bt)$ for some real number t.

Proof: If $(x, y) = (at, bt)$ then $bx - ay = 0$, which is a line through the origin with slope b/a. Let L be the line $Ax + By = 0$ for real numbers A, B not both 0.
If $B = 0$, the line is vertical without a rational slope.
If $B \neq 0$, then the slope is $-A/B$ and we can write $-A/B = a/b$ for integers a, b. Now (x, y) lies on L if and only if $bx - ay = 0$, which is $(x, y) = (at, bt)$. ☒

Definition: The **unit circle** is the set $\{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$

Theorem 8.12 (Parametrization of the Unit Circle): If $x \neq -1$, then $x^2 + y^2 = 1$ if and only if there is a real number t such that $(x, y) = \left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2}\right)$

Further, such a point (x, y) has rational coordinates if and only if t is a rational number.

Irrational Numbers

Theorem 8.14: The positive integer K has no rational square root if K is not the square of an integer.

Proof: We use contradiction.
Suppose $\sqrt{K}$ is rational and that m/n is a fraction representing it, where n is positive and minimal. If m/n is not an integer, then there's an integer q such that $m/n - 1 < q < m/n$ so $0 < m - nq < n$.
Since $m - nq \neq 0$

$$\frac{m}{n} = \frac{m(m - nq)}{n(m - nq)} = \frac{m^2 - mnq}{n(m - nq)} = \frac{n^2K - mnq}{n(m - nq)} = \frac{nK - mq}{m - nq}$$

since $0 < m - nq < n$, we found a representation with a smaller positive denominator so if the square root of K is rational, it must be an integer. ☒

Theorem 8.16 (Rational Zeros Theorem): Let $c_0, \ldots, c_n$ be integers with $n \geq 1$ and $c_0, c_n \neq 0$, and let $f(x) = \sum_{i=0}^{n} c_i x^i$ for $x \in \mathbb{R}$.

If r is a rational solution to the equation $f(x) = 0$, written as p/q in lowest terms, then p must divide c_0 and q must divide c_n.

Proof: When $f(r) = 0$ then we can get

$$\sum_{i=0}^{n} c_i p^i q^{n-i} = 0 \Rightarrow -c_n p^n = \sum_{i=0}^{n-1} c_i p^i q^{n-1} = q \sum_{i=0}^{n-1} c_i p^i q^{n-1-i}$$

Since q divides one side, it must divide the other. Since q and p are relatively prime (as p/q is lowest terms) then q must divide c_n. similarly, for

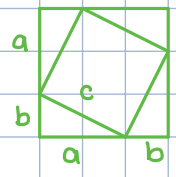
$$-c_0 q^n = \sum_{i=1}^{n} c_i p^i q^{n-i} = p \sum_{i=1}^{n} c_i p^{i-1} q^{n-i}$$

so p divides c_0 ☒

Example: If the equation $x^3 - 6 = 0$ has a rational solution r, written p/q, then q must divide 1 and p must divide 6 so the only possibilities are $r = \pm 1, \pm 2, \pm 3, \pm 6$ and none work.

Pythagorean Triples

Theorem 8.20 (Pythagorean Theorem): If a, b, c are the lengths of the sides of a right triangle with c the length of the side opposite the right angle, then $a^2 + b^2 = c^2$.



$(a+b)^2 = c^2 + 4(ab/2) \Rightarrow a^2 + b^2 = c^2$ ☒

Definition: The integer solutions to $a^2 + b^2 = c^2$ are called Pythagorean triples

Examples: $(3,4,5)$; $(5,12,13)$; $(8,15,17)$; $(7,24,25)$; $(20,21,29)$; $(9,40,41)$

Theorem 8.22: The Pythagorean triples are the integer multiples of triples of the form $(2rs, r^2 - s^2, r^2 + s^2)$ or $(r^2 - s^2, 2rs, r^2 + s^2)$ where r, s are integers.