1 The Foundations: Logic and Proofs

Consider the following argument:

> i eat chocolate if i am depressed
> i am not depressed
> therefore i am not eating chocolate

Obviously, the logic is flawed. . . but how do we write this in a more formal way?

1.1 Propositional Logic

A *statement* is a senetence or mathematical expression that is either *true* or *false*—e.g.

- P : The number 3 is odd
- Q : The number 6 is even
- R : The number 4 is odd

Not a statement

- $x > 2$ (the true value depends on x)
- $x = 2,\ t + 4q = 17$

Combining statements

Given statements P and Q:

- "P and Q" is a statement ($P \wedge Q$)
- "P or Q" is a statement ($P \vee Q$)

We can construct a truth table to represent the truth values of $P \wedge Q$ and $P \vee Q$:

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

Table 1: Truth tables for conjunction ($\wedge$) and disjunction ($\vee$)

Conditional Statements

The expression:

If P, then Q (or $P \Rightarrow Q$)

is a *conditional statement.*

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

Table 2: Truth table for conditional statements

Example:

$P(n)$: The integer n is odd
$Q(n)$: The integer n^2 is odd

$P(n)$ and $Q(n)$ are not statements, but they are *predicates* (statements once n is determined). So the conditional statement is

$P(n) \Rightarrow Q(n)$: If the integer n is odd, then the integer n^2 is odd

Proving a statement of the form $P \Rightarrow Q$

1. Direct proof: Assume P is true and "prove" that Q is also true

Example: Let's construct a truth table for $(P \vee Q) \Rightarrow R$

P	Q	R	$P \vee Q$	$(P \vee Q) \Rightarrow R$
T	T	T	T	T
T	F	T	T	T
T	F	F	T	F
F	T	T	T	T
F	F	T	F	T
F	F	F	F	T

Table 3: Truth table for $(P \vee Q) \Rightarrow R$

Where we want to prove

If n is odd, then n^2 is odd.

The first proposition is symbolically $O(n) : n$ is odd, and the conditional statement is

$$O(n) \Rightarrow O(n^2)$$

Def First we define and integer n odd if $n = 2k + 1$ for some integer k. An integer is even if $n = 2k$ for some integer k.

Remark. *The set of integers*

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

where k is an integer is denoted as $k \in \mathbb{Z}$.

Proof Suppose n is odd. So by definition, $n = 2k + 1$ for some $k \in \mathbb{Z}$.

$$\implies n^2 = (2k + 1)(2k + 1) = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

Since $2k^2 + 2k$ is an integer, we have that n^2 is in fact odd. $\square$

Another Example (Because students love examples) Suppose x and y are positive numbers. Prove that if $x < y$ then $x^2 < y^2$.

Sol Suppose x and y are positive real numbers and further suppose that $x < y$. A fundamental property of $<$ on the real numbers is that if $a < b$ and $c > 0$, then $a \cdot c < b \cdot c$ since if

$$a < b \implies 0 < b - a$$

and the product of the two positve numbers is positive, i.e.

$$0 < c(b - a) = cb - ca$$

Which now implies $ca < cb$. In this case, if $a = x, b = y, c = x$, then

$$x^2 = x \cdot x < x \cdot y$$

Now if we swap and use $c = y$, we have

$$x \cdot y < y \cdot y = y^2$$

Concatenating the two inequalities, we find that

$$x^2 = x \cdot x < x \cdot y < y \cdot y = y^2$$

Because x and y were arbitrary positive numbers, the conclusion holds. $\square$

1.2 Logical Equivalence

Two statements are *logically equivalent* if they have the same truth value, e.g. x & y are real numbers

$P:\ x \cdot y = 0$

$Q:\ x = 0$ or $y = 0$

are equivalence since they are either both T or both F.

If P and Q are equivalent we say P if and only if Q and we write

$$P \iff Q \quad \text{or} \quad P \equiv Q$$

which is a *biconditional statement*. Note that P & Q are predicates but $P \iff Q$ is a statement.

Example P, Q, and R are statements

$$((P \vee Q) \Rightarrow R) \iff ((P \Rightarrow R)) \wedge (Q \Rightarrow R)$$

P	Q	R	$P \vee Q$	$P \Rightarrow R$	$Q \Rightarrow R$	$(P \vee Q) \Rightarrow R$	$(P \Rightarrow R) \wedge (Q \Rightarrow R)$
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	F
T	F	T	T	T	T	T	T
T	F	F	T	F	T	F	F

Table 4: Truth table

Contrapositive The *contrapositive* state is

If not Q, then not P

Claim The statement $P \Rightarrow Q$ and its contrapositive $\neg Q \Rightarrow \neg P$ are logically equivalent.

Proof For fun watch the YouTube video Not Knot

P	Q	$P \Rightarrow Q$	$\neg Q$	$\neg P$	$\neg Q \Rightarrow \neg P$
T	T	T	F	F	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

Table 5: Truth table proof

Remark A proof of a condition statement by proving the contrapositive is called a *contrapositive proof.*

Example Let's prove the statement

Suppose x is a real number. If $x^2 + 5x < 0$, then $x < 0$

using a contrapositive proof.

Proof

$$P : x^2 + 5x < 0$$
$$Q : x < 0$$

So $\neg Q \Rightarrow \neg P$ is

If $x \geq 0$, then $x^2 + 5x \geq 0$

Suppose x is a real number satisfying $x \geq 0$. Then $5x \geq 0$ & $x^2 \geq 0$. Thus

$$x^2 + 5x \geq 0$$

Because $x \geq 0$ was arbitrary, we have $\neg Q \Rightarrow \neg P$.

Converse $Q \Rightarrow P$ is called the *converse* of $P \Rightarrow Q$.

Example

P: f is differentiable at $x = 0$

Q: f is continuous at $x = 0$

As an example, $f = |x|$ is continuous at $x = 0$ but not differentiable at $x = 0$—so here

$P \Rightarrow Q$ is true, but
$Q \Rightarrow P$ is false

Another example is

P: A is an invertible 2×2 matrix
Q: $\det A \neq 0$

Negation & Quantifiers

Example Let m and n be integers. If 4 divides the product mn (results in an integer), then 4 divides m or 4 divides n.

- Converse: If 4 divides m or 4 divides n, then 4 divides mn
- Contrapositive: If 4 does not divide m and 4 does not divide n, then 4 does not divide mn

This statement is False!

Proof If $m = n = 2$, then 4 divides $mn = 4$. But 4 does *not* divide m or n, thus the statement is F. $\square$

The *negation* of a statement P is the statement whose truth values are opposite for those of P and is denoted as $\neg P$.

Claim Let P and Q be statements.

The negation of the conditional statement $P \Rightarrow Q$ is $P \wedge (\neg Q)$.

Proof We check that $\neg(P \Rightarrow Q)$ and $P \wedge (\neg Q)$ are logically equivalent with a truth table.

P	Q	$P \Rightarrow Q$	$\neg(P \Rightarrow Q)$	$\neg Q$	$P \wedge (\neg Q)$
T	T	T	F	F	F
T	F	F	T	T	T
F	T	T	F	F	F
F	F	T	F	T	F

Table 6: Truth table for negation of a conditional statement

Discussion Let P and Q be statements and negate $P \vee Q$, and find what it is equivalent to.

P	Q	$P \vee Q$	$\neg(P \vee Q)$	$\neg P \wedge \neg Q$
T	T	T	F	F
T	F	T	F	F
F	T	T	F	F
F	F	F	T	T

Table 7: Truth table for negation of a disjunction

So the two statements are logically equivalent $\neg(P \vee Q) \iff \neg P \wedge \neg Q$. This is one of De Morgan's Laws:

$$\neg(P \vee Q) \iff \neg P \wedge \neg Q$$
$$\neg(P \wedge Q) \iff \neg P \vee \neg Q$$

Table 8: De Morgan's Laws

Example Every nonempty subset of $\mathbb{N}$ has a smallest element.

Notation $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ is the set of natural numbers.

Definition The symbols $\forall$ and $\exists$ are called *quantifiers*.

- $\forall$ stands for "for all" or "for every"
- $\exists$ stands for "there exists" or "there is"

thus we write the above statement as logical mathematical symbols is

$$\forall X \subset \mathbb{N} \text{ with } X \neq \phi, \exists x_0 \in X \text{ such that } x_0 \leq x \quad \forall x \in X$$

HW NOTES

$$(P \Leftrightarrow Q) \equiv [(P \Rightarrow Q) \wedge (Q \Rightarrow P)]$$

Show both $P \Rightarrow Q$ and $Q \Rightarrow P$ are true.

Example Negate the statemen:

The integers 5 and 9 are both odd.

Using De Morgan's Laws $\neg(P \wedge Q) \equiv \neg P \vee \neg Q$ we can rewrite the statement as

Either 5 is even or 9 is even.

Let A be a set and $a \in A$.

- $\forall a \in A, P(a)$: means $P(a)$ is true for every element of set A.
- $\exists a \in A, P(a)$: means $P(a)$ is true for some element of set A.
- $\neg(\forall a \in A, P(a)) \equiv \exists a \in A, \neg P(a)$
- $\neg(\exists a \in A, P(a)) \equiv \forall a \in A, \neg P(a)$

WARNING :

- $\neg(a \in A) \equiv a \notin A$ is not the same as
- $\neg(\forall a \in A) \equiv \exists a \in A$

Example Let $C(x)$: x has taken calculus (x is a 310 student).

$G(x, y)$: $x > y$ $(x, y \in \mathbb{R})$
$P(x)$: x is prime $(x \in \mathbb{N} = \{0, 1, 2, \ldots\})$

1. $\forall x, C(x)$ as a statement: Every 310 student has taken calculus
   Negation: There is some 310 student who has not taken calculus, or
2. $\exists x, C(x)$
3. Negate $\forall x \in \mathbb{N}, \neg P(x)$

   Statement: Every natural number is not prime.
   Negation: $\exists x \in \mathbb{N}, P(x)$—There exist a natural number that is prime.
4. Negate $\exists x \in \mathbb{R}, G(x, 2)$

   Statement: There exists a real number greater than 2.
   Negation: $\forall x \in \mathbb{R}, \neg G(x, 2)$—Every real number is less than or equal to 2. $\Longleftrightarrow$

Example Negate the following statements:

1. For all $X \subseteq \mathbb{N}$, there exists an integer n such that $|X| = n$.

   Symbolically: $\forall X \subseteq \mathbb{N} \quad \exists n \in \mathbb{Z}, \quad |X| = n$. Where $|X|$ is "the number of elements in the set X, cardinality of X".

   e.g.

   - $X = \{1, 2, 3\}$ then $|X| = 3$
   - All even natural numbers $X = \{0, 2, 4, 6, 8, \dots\}$
     then $|X| = \infty$, so $\nexists$ an integer n such that $|X| = n$.

   Thus the negatation $\exists X \subseteq \mathbb{N} \quad \forall n \in \mathbb{Z}, \quad |X| \neq n$ shows that the statement is <u>false</u>.

2. There exists $x \in \mathbb{Z}$ such that for all $n \in \mathbb{Z}, \quad x \neq n + 2$.

   Symbolically: $\exists x \in \mathbb{Z} \quad \forall n \in \mathbb{Z}, \quad x \neq n + 2$.

   Negation: $\forall x \in \mathbb{Z} \ \exists n \in \mathbb{Z}, \quad x = n + 2$.

   which is <u>true</u>.

3. For all $x \in \mathbb{R}$, there exists $y \in \mathbb{R}$ such that $y^3 = x$.

   ...this is <u>true</u>

4. There exists $x \in \mathbb{Z}$ such that for all $n \in \mathbb{Z}, \quad x \neq n + 2$.

   ...this is <u>false</u>.

Example True or False; Negate

1. For all $x \in \mathbb{R}$, there exists $y \in \mathbb{R}$ such that $y^2 = x$

$$\forall x \in \mathbb{R}\ \exists y \in \mathbb{R},\ \ y^2 = x$$

   Negation: $\exists x \in \mathbb{R}\ \forall y \in \mathbb{R},\ \ y^2 \neq x$

   There exists $x \in \mathbb{R}$ so that for all $y \in \mathbb{R}$, $y^2 \neq x$

   The original statement is <u>false</u>:

   Let $x = -1$. Then $y^2 \neq -1\ \ \forall y \in \mathbb{R}$

2. For all $x \in \mathbb{R}$, there exists $y \in \mathbb{R}$ such that $y^3 = x$.

$$\forall x \in \mathbb{R}\ \exists y \in \mathbb{R},\ \ y^3 = x$$

   Negation: $\exists x \in \mathbb{R}\ \forall y \in \mathbb{R},\ \ y^3 \neq x$

   The original statement is <u>true</u> because every real number has a cube root.

Definition A *set* is a collection of objects.
The objects in a set are called *elements.*

Definition The unique set containing no elements is called the *empty set*, denoted by $\emptyset$ or $\varnothing$.

Example $A = \{1, 2, 3, 4, 5, \{6, 7\}\}$

(a) $1 \in A$ (1 is an element of A) T

(b) $\{1\} \in A$ F

(c) $1 \subseteq A$ F

(d) $\{1\} \subseteq A$ F

(e) $\{6, 7\} \subseteq A$ F

(e)' $\{\{6, 7\}\} \subseteq A$ T

(f) $\{4, 5\} \subseteq A$ T

(g) $|A| = 6$ T

(h) $\emptyset \in A$ F

Set-builder notation used to describe sets when its difficult to list all elements.

Example Even integers $\{\dots, -4, -2, 0, 2, 4, \dots\}$

$$= \{2k \mid k \in \mathbb{Z}\} = \{2k : k \in \mathbb{Z}\}$$

Example The set of rational numbers

$$\mathbb{Q} := \left\{ \frac{P}{q} \mid p, q \in \mathbb{Z},\ q \neq 0 \right\}$$

The set of *irrational numbers* is set of all real numbers that are not rational.

Remark $\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R}$

Example Write in set-builder notation:

1. $\left\{\dots, \frac{1}{27}, \frac{1}{9}, 1, 3, 9, 27 \dots\right\}$

$$= \{3^k \mid k \in \mathbb{Z}\}$$

2. The set of odd integers

$$\{2k + 1 \mid k \in \mathbb{Z}\}$$

3. $(-\infty, 3] = \{x \in \mathbb{R} \mid x \leq x\}$

Definition Let A and B be sets.

- *Union*: $A \cup B := \{x \mid x \in A \vee x \in B\}$
- *Intersection*: $A \cap B := \{x \mid x \in A \wedge x \in B\}$
  Definition: The sets A and B are *disjoint* if $A \cap B = \emptyset$. $\varnothing$
- *Set-difference*: $A - B = A \setminus B := \{x \in A \mid x \notin B\}$
- The *compliment* of A in a set U is $A^c = \overline{A} := \{x \in U \mid x \notin a\}$
- *Cartesian product*:

$$A \times B := \{(a, b) \mid a \in A, b \in B\}$$

(e.g. $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$)

T/F

1. $A \times B = B \times A$
   F: $A = \{1\},\ B = \{2\}$, so $A \times B = \{(1, 2)\}$ but $B \times A = \{(2, 1)\}$
2. If $|A| = 2$ and $|B| = 3$, then $|A \times B| = 6$ T
3. $\mathbb{R} \subseteq \mathbb{R}^2$ F

4'. $\mathbb{R} \times \{O\} = \mathbb{R}^2$ T

Example Write out the sets by listing all elements:

1. $\{x \in \mathbb{R} \mid \cos(x) = 0,\, 0 \leq x \leq 2\pi\}$
$$= \left\{\frac{\pi}{2}, \frac{3\pi}{2}\right\}$$
2. $\{x \in \mathbb{R} \mid \sin(x) = 0,\, 0 \leq x \leq 2\pi\}$
$$= \{0, \pi, 2\pi\}$$
3. $\{m \mid m \in \mathbb{N},\, m^2 < 10\}$
$$= \{1, 2, 3, 0\}$$

Example Compute the following sets:

1. $\bigcup\limits_{n\in\mathbb{N}} \left[\frac{1}{n+1}, n+1\right] = (0, \infty)$

   Looking at a few of our favorite natural numbers...
   - $n = 4$: $\left[\frac{1}{5}, 5\right]$
   - $n = 0$: $[1, 1] = \{1\}$
   - $n = 2$: $\left[\frac{1}{3}, 3\right]$

   So the union of all these sets is $(0, \infty)$.
2. $\bigcap\limits_{n\in\mathbb{N}} \left[\frac{1}{n+1}, n+1\right] = \{1\}$

   The intersection of all these sets is when $n = 0$ because that is when the two values are equal to each other.

Claim Let A, B, and C be sets.
If $B \subseteq C$, then $A \times B \subseteq A \times C$.

Proof. Let $(a, b) \in A \times B$. By definition of the Cartesian product, $a \in A$ and $b \in B$. Since $B \subseteq C$, $b \in C$. Thus, $(a, b) \in A \times C$. □

Claim For all sets A and B, $(A \cup B)^c = A^c \cap B^c$.

Proof. ($\subseteq$) Let $x \in (A \cup B)^c$.
This implies $x \notin A$ and $x \notin B$. Thus, $x \in A^c$ and $x \in B^c$ so $x \in A^c \cap B^c$.

($\supseteq$) Let $x \in A^c \cap B^c$, so $x \notin A$ and $x \notin B$.
This implies x is not in A or B. Thus, $x \notin A \cup B$ so $(A \cup B)^c$. □

Claim $\mathbb{Z} = \{25a + 24b \mid a, b \in \mathbb{Z}\}$.

Proof. ($\supseteq$) This is obvious, since $25a + 24b \in \mathbb{Z}$ for all $a, b \in \mathbb{Z}$.

($\subseteq$) Let $k \in \mathbb{Z}$. Set $a = k$ and $b = -k$. Then $25a + 24b = 25k - 24k = k$. □

To get to the forwards proof we can test a few values of k to find anything:

- $k = 0$: $25(0) + 24(0) = 0$
- $k = 1$: $25(1) + 24(-1) = 1$
- $k = 2$: $25(2) + 24(-2) = 2$... so we can see the pattern
- $k = 25k + 24(-k)$

1.3 Proof by Contradiction

Example Suppose A, B, and C are nonempty sets

T/F: If $A \times B = A \times C$ then $B = C$
True

Note: $A = \emptyset$

$$A \times B = \emptyset = A \times C$$

for all B, C

Proof. $(B \subseteq C)$ Let $b \in B$. ~~Suppose $a \in A$~~ Since $A = \emptyset$, there is an element $a \in A$. Then

$$(a, b) \in A \times B$$

Since $A \times B = A \times C$, we know

$$(a, b) \in A \times C$$

By definition of the Cartesian product, $b \in C$. This proves $B \subseteq C$

$(C \subseteq B)$ By similar reasoning (with the roles of B and C reversed), we can show $C \subseteq B$. □

Example Prove that if $a, b \in \mathbb{Z}$, then $a^2 \neq 4b + 2$.

Ideas

1. Cases: a is odd vs. a is even

$$a = 2k$$

2. looking at all the squares

$$c_0 = 0^2 = 0, \quad c_1 = 1^2 = 1, \quad 2^2 = 4, \quad 3^2 = 9, \quad 4^2 = 16, \quad 5^2 = 25 \ldots$$

which can be written as

$$c_n = c_{n-1} + (n-1)(2k+1)$$

3. Claim: The prod of odd numbers is odd and the prod of even numbers is even.

$$a^2 = 4b + 2 = 2(2b + 1)$$

So if a^2 is even $\Rightarrow$ a is even: $a = 2k$

$$\begin{aligned} (2k)^2 &= 2(2b+1) \\ \implies 4k^2 &= 2(2b+1) \\ \implies 2k^2 &= 2b + 1 \end{aligned}$$

where the RHS is odd but the LHS is even, which is a contradiction.

Proof. (Contradiction) Asume there exist $a, b \in \mathbb{Z}$ such that $a^2 = 4b + 2$. Then a^2 is even, so a is even. Write $a = 2k$ for some $k \in \mathbb{Z}$.
Then

$$(2k)^2 = 4b + 2 \implies 2k^2 = 2b + 1$$

THe LHS of the equation is even, while the RHS is odd. This is a contradiction. □

Suppose you want to prove statement $P \ldots$

Proof by Contradiction Steps

1. Assume $\neg P$
2. Show that $\neg P$ implies that there is some statement C so that $C \wedge \neg P$ (Contradiction)
3. $\neg P$ is False $\Leftrightarrow$ P is True

Proposition The number $\sqrt{2}$ is irrational.

Ideas

$$\begin{aligned} \sqrt{2} = \frac{a}{b} &\implies \sqrt{2}b = a \\ &\implies 2b^2 = a^2 \end{aligned}$$

a^2 is even $\implies a = 2k$

$$\begin{aligned} &\implies 2b^2 = (2k)^2 \\ &\implies b^2 = 2k^2 \end{aligned}$$

b^2 is even $\implies b = 2l$

Proof. (Contradiction) Assume $\sqrt{2}$ is rational. Thus there are integers $a, b \in \mathbb{Z}$, $b \neq 0$ so that $\sqrt{2} = \frac{a}{b}$. We can assume a and b have no common factors—that is, there is no positive integer greater than 1 that divides both a and b. Now,

$$\sqrt{2} = \frac{a}{b} \implies \sqrt{2}b = 2 \implies 2b^2 = a^2$$

So a^2 is even, and thus a is even. Write $a = 2k$ for some $k \in \mathbb{Z}$. Then the equation becomes:

$$2b^2 = (2k)^2 \implies 2b^2 = 2k,$$

so b^2 is even, and thus b is also even.

Thus both a and b are even, which contradicts our earlier assumption that they have no common factors. □

Example

1. Prove there is no integer x such that

$$x^2 = 5 \quad \text{and} \quad x^2 = 9$$

2. Suppose a, b are nonzero. Prove that if ab is irrational, then a is irrational or b is irrational.

Example Prove that for any integer n,

$$n^2 = 4k \quad \text{or} \quad n^2 = 4k+1 \quad \text{for some} \quad k \in \mathbb{Z}$$

Proof. If n is even, then $n = 2m$ for some $m \in Z$. Then $n^2 = (2m)^2 = 4m^2$ so if $k = m^2$, the claim holds.

If n is odd, $n = 2m+1$ for some $m \in \mathbb{Z}$. Then $n^2 = (2m+1)^2 = 4m^2 + 4m + 1 = 4(m^2 + m) + 1$. If $k = m^2 + m$, the claim holds. □

Definition. *Given $a, b \in \mathbb{Z}$, we say a divides $b(a \mid b)$ if $b = ak$ for some $k \in \mathbb{Z}$.*

Example $2 \mid 12$, $3 \mid 27$, $3 \nmid 10$

Example Let $a, b, c \in \mathbb{Z}$ Prove that if $a \mid b$ and $b \mid c$ then $a \mid c$.

Proof. Since $a \mid b$ and $b \mid c$, there exists $k, l \in \mathbb{Z}$ such that $b = ak$ and $c = bl$. Thus $c = (ak)l = a(kl)$. Since $kl \in \mathbb{Z}$, $a \mid c$. □

Recall $\mathbb{N} = \{0, 1, 2, 3, \ldots\} \subseteq \mathbb{Z}$

Well-ordering Principle: Every nonempty subset of $\mathbb{N}$ has a smallest element.

Theorem. *Division Algorithm: Let $a, b \in \mathbb{Z}$ with $b > 0$. <u>There exists</u> <u>unique</u> integers q and r such that:*

$$a = qb + r, \quad 0 \leq r < b.$$

Proof. Let $a, b \in Z$ with $b > 0$.

Consider the set

$$A = \{a - xb \mid x \in \mathbb{Z},\, a - xb \geq 0\}$$

The set A is nonempty: If $a \geq 0$, then $a \in A$. If $a < 0$, then $a - ab \in A$ since $a - ab = a(1-b)$ where $b > 0 \Rightarrow b \geq 1 \Rightarrow (1-b) \leq 0$.

By the well-ordering principle, A has a smallest element, call it r. Since $r \in A$, there exists $q \in \mathbb{Z}$ such that $r = a - qb$. Thus $a = qb + r$.

Since $r \in A$, $r \geq 0$. We want to show $r < b$. If not, $r \geq b$ and:

$$r - b = a - qb - b = a - (q+1)b \geq 0$$

so $r - b \in A$. This contradicts our choice of r as the smallest element of A, so $r < b$.

To prove r and q are unique let $q_1, r_1 \in \mathbb{Z}$ such that $a = q_1 b + r_1$ and $0 \leq r_1 \leq b$. We have:

$$\begin{aligned} 0 = a - a &= (qb + r) - (q_1 b + r_1) \\ &= (q - q_1)b + (r - r_1) \\ \implies r - r_1 &= (q_1 - q)b \end{aligned}$$

We may assume $r \geq r_1$, so $r - r_1 \geq 0$.

Further, $r < b$ so $r - r_1 < b$. But $r - r_1 = (q_1 - q)b$ implies that $r - r_1 \geq b$, because $r - r_1$ is a multiple of b. Thus $0 \leq r - r_1 < b$, so since $r - r_1$ is a multiple of b, it must be zero. Thus $r = r_1$ and thus $0 = (q_1 - q)b \Rightarrow q_1 = q$. □

Example If $5 \nmid n$, then the ones digit of n^2 is not 5. From the division algorithm

$$n = 5q + r, \quad r \in \{1, 2, 3, 4\}$$

Looking at some examples:

$$\begin{aligned} n = 5q + 1 \implies n^2 &= 25q^2 + 10q + 1 \\ &= 5(5q^2 + 2q) + 1 \\ n = 5q + 3 \implies n^2 &= 25q^2 + 30q + 9 \\ &= 5(5q^2 + 6q + 1) + 4 \end{aligned}$$

Week 4

Recall Given $a, b \in \mathbb{Z}$ a divides b or $a \mid b$. This means there is some integer c such that $b = ac$.

Warm-up T or F

Let a, b, m be integers and $m \neq 0$. If $ma \mid mb$, then $a \mid b$.

Proof. $ma \mid mb$ implies that $mb = mac$ for some integer c. Because $m \neq 0$ (dividing both side), we get $b = ac$ which is equivalent to $a \mid b$. □

Definition For integers a, b, d if $d \mid a$, we say d is a divisor of a. If $d \mid a$ and $d \mid b$, we say d is a common divisor of a, b (with $|d| \leq |a|$, $|d| \leq |b|$).

If d is the largest positive integer that divides both a and b we call d the greatest common divisor of a, b.

$$d = \gcd(a, b)$$

Example: $\gcd(2, 3) = 1, \quad \gcd(9, 12) = 3$

The Euclidean Algorithm

Input: a, b positive integers
Output: γ_n positive integer
Claim: $\gamma_n = \gcd(a, b)$

where we repeatedly apply the division algorithm to find the gcd.

Assume $a < b$

$$\begin{aligned} b &= q_1 a + \gamma_1 \quad \text{where} \quad 0 \leq \gamma_1 < a \\ a &= q_2 \gamma_1 + \gamma_2 \quad \text{where} \quad 0 \leq \gamma_2 < \gamma_1 \end{aligned}$$

e.g $\gcd(5817, 1428)$:

$$\begin{array}{r} 4 \\ 1428\overline{)5817} \\ \underline{5712} \\ 105 \end{array} \quad , \quad \begin{array}{r} 13 \\ 105\overline{)1428} \\ \underline{105} \\ 378 \\ \underline{315} \\ 63 \end{array}$$

So

$$\begin{aligned} a = 1428&, \quad b = 5817 \\ 5817 &= 4 \cdot 1428 + 105 \\ 1428 &= 13 \cdot 105 + 63 \\ 105 &= 1 \cdot 63 + 42 \\ 63 &= 1 \cdot 42 + 21 \\ 42 &= 2 \cdot 21 + 0 \end{aligned}$$

Thus the claim $\gcd(5817, 1428) = 21$. Or in symobolic form:

$$\begin{aligned} \gamma_1 &= q_3 \gamma_2 + \gamma_3 \quad \text{where} \quad 0 \leq \gamma_3 < \gamma_2 \\ &\vdots \\ \gamma_{n-2} &= q_n \gamma n - 1 + \gamma_n \quad \text{where} \quad 0 \leq \gamma_n < \gamma_{n-1} \\ \gamma_{n-1} &= q_{n+1} \gamma_n + 0 \end{aligned}$$

Theorem. $\gamma_n = \gcd(a, b)$

Proof. Step 1: We will prove $\gamma_n \geq \gcd(a, b)$.

To show $\gamma_n \geq d$, we will prove $d \mid \gamma_n$. By definition, $d \mid a$ and $d \mid b$. Because $\gamma_1 = b - q_1 a$, so $d \mid \gamma_1$. Because $\gamma_2 = a - q_2\gamma_1$, so $d \mid \gamma_2$. With the same argument we conclude $d \mid \gamma_n$.

Step 2: We will prove $\gamma_n \leq d = \gcd(a, b)$. We need to show $\gamma_n \mid a$ and $\gamma_n \mid b$. From $\gamma_1 = q_{n+1}\gamma_n$, we get $\gamma_n \mid \gamma_{n-1}$. From $\gamma_2 = q_n\gamma_{n-1} + \gamma_n$, we get $\gamma_n \mid \gamma_2$. With the same argument, we get $\gamma_n \mid \gamma_1$ and $\gamma_n \mid \gamma_2$ which implies $\gamma_n \mid a$ and $\gamma_n \mid b$. □

Theorem. *(Bezout's Identity) There exists such integers s, t such that*

$$\gcd(a, b) = as + bt$$

e.g. $\gcd(5, 7) = 1$ and from the identity:

$$1 = 5 \cdot 3 + 7 \cdot (-2)$$

From our previous example $\gcd(5817, 1428) = 21$ and from the identity:

$$21 = 5817s + 1428t$$

Using the Euclidean Algorithm we can do the following:

$$\begin{aligned}
21 &= 63 - 42 \\
&= 63 - (105 - 63) \\
&= -104 + 2(1428 - 13 \cdot 105) \\
&= 2 \cdot 1428 - 27(5817 - 4 \cdot 1428) \\
&= -27 \cdot 5817 + 110 \cdot 1428
\end{aligned}$$

where $s = -27$ and $t = 110$.