Louis Meunier

Algebra I, II MATH235

Course Outline:

Introductory abstract algebra. Sets, functions, relations. Methods of proof. Arithmetic on integers. Fields, rings; groups, subgroups, cosets.

Contents

I. Fundamentals

“It is intuitively obvious.” - Anonymous

“Trivial” - Anonymous

1 Sets

1.1 Definition

A **set** can be considered as a collection of elements; more intuitively, you can consider something a set if you can determine whether a given object belongs to it. Typically sets are defined as $A = \{1, 2, \dots\}$, by a property $A = \{x \,|\, x\%2 = 0\}$, or with an appropriate verbal description.

1.2 Set operations

There are a number of ways to “combine” sets:

- **Union**: $A \cup B = \{x \,|\, x \in A \text{ or } x \in B\}$
- **Intersection**: $A \cap B = \{x \,|\, x \in A \text{ and } x \in B\}$
- **Difference**: $A \setminus B = \{x \,|\, x \in A \text{ and } x \notin B\}$

Lemma 1.1. $A = (A \setminus B) \cup (A \cap B)$

Proof. To prove set equivalencies, we must prove that both RHS $\subseteq$ LHS and LHS $\subseteq$ RHS; meaning, the LHS and RHS are subsets of each other, and are thus equal.

First, to prove LHS $\subseteq$ RHS, let $a \in A$. If $a \notin B$, then $a \in A \setminus B$, and $a \in$ RHS. Else, if $a \in B$, then $a \in A \cap B$ and $a \in$ RHS. Thus, LHS $\subseteq$ RHS.

Next, to prove RHS $\subseteq$ LHS, let $a \in$ RHS. If $a \in A \setminus B$, then $a \in A =$ LHS. Else, $a \in A \cap B$, and thus $a \in A =$ LHS. Thus, RHS $\subseteq$ LHS. Since LHS $\subseteq$ RHS and RHS $\subseteq$ LHS, LHS = RHS. ■

1.3 Indexed sets

Let I be a set. If for every $i \in I$, we have a set B_i, we say that we have a *collection* of sets B_i indexed by I. We write $\{B_i : i \in I\}$.

Example 1.1. *Let $I = \{1, 2, 3\}$, and $B_i = \{1, 2, 3, 4\} \setminus \{i\}$ (B_i is the set of all numbers from 1 to 4, excluding i), for $i \in I$. We thus have $B_1 = \{2, 3, 4\}$ (etc.).*

This concept of indexing allows us to introduce repeated unions/intersections. For instance, we can write

$$\bigcup_{i \in I} B_i = B_1 \cup B_2 \cup B_3 = \{1, 2, 3, 4\}.$$

Similarly,

$$\bigcap_{i \in I} B_i = \{4\}.^{1}$$

Example 1.2. *Let $I = \mathbb{R}$, and $B_i = [i, \infty] = \{r \in \mathbb{R} : r \geq i\}$. Then, $\bigcup_{i \in \mathbb{R}} B_i = \mathbb{R}$ and $\bigcap_{i \in \mathbb{R}} B_i = \emptyset$.*

1.4 Cartesian product

Let $A_1, A_2, \ldots, A_n$ be sets. We define the **Cartesian product**

$$A_1 \times A_2 \times \cdots \times A_n = \{(x_1, x_2, \ldots, x_n) : x_i \in A_i, \text{ for } 1 \leq i \leq n\}.$$

For instance,

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

Example 1.3. *Let $A = B = \mathbb{R}$. $A \times B = \{(x, y) : x \in \mathbb{R}, y \in \mathbb{R}\} = \mathbb{R}^2$ is the set of all points in the Cartesian plane.*

We can also define Cartesian products over an index set. Let I be an index set, with A_i for all $i \in I$. Then, we can write

$$\prod_{i \in I} A_i = \{(a_i)_{i \in I} : a_i \in A_i\}$$

[1] You can somewhat consider these "large" unions/intersections as analogous to summations Σ and products Π.

Example 1.4.

$$I = \mathbb{N}, A_0 = \{0, 1, 2, \dots\}, A_1 = \{1, 2, 3, \dots\}, ..., A_i = \{i, i+1, i+2, \dots\}$$
$$Y := \prod_{i \in I} A_i = \{(a_0, a_1, a_2, \dots) : a_i \in \mathbb{N}, a_i \geq i\}$$

We can say that a particular vector $(b_0, b_1, \dots) \in Y$ if for each b_i, $b_i \geq i$ (and $b_i \in \mathbb{N}$, of course). In other words, a particular item of the vector must be greater than or equal to its index. Thus, we can say

$$(0, 1, 2, 3, \dots) \in Y$$

while

$$(2, 2, 2, 2, \dots) \notin Y$$

since $a_3 = 2 \implies i = 3$, and $2 \ngeq 3$.

2 Methods of Proof

2.1 Proving equality via two inequalities

In short, say $x, y \in \mathbb{R}$. $x = y \iff x \leq y$ and $y \leq x$. Similarly, in the context of sets, we can say that, for two sets X, Y, $X = Y \iff X \subseteq Y$ and $Y \subseteq X$.

2.2 Contradiction (bwoc)

Given a statement P, we can prove P true by assuming P false ($\equiv \neg P$), then arriving to a contradiction (this contradiction is often a violated axiom or basic rule of the system at hand.)

Example 2.1. *Show that there are no solutions to $x^2 - y^2 = 1$ in the positive integers.*

Proof (bwoc). Assume there are, so $x, y \in \mathbb{Z}_+$.[2]We can then write

$$1 = x^2 - y^2 = (x - y)(x + y).$$

$x - y$ and $x + y$ must be integers, and so we have two cases, $\begin{cases} x - y = 1 \\ x + y = 1 \end{cases}$ and $\begin{cases} x - y = -1 \\ x + y = -1 \end{cases}$. In either case, y must be zero, contradicting our initial assumption and thus proving the statement. ■

[2] $\mathbb{Z}_+$ is used to denote positive integers; similarly, $\mathbb{Z}_-$ denotes negative integers.

2.3 Proving the contrapositive

Logically, $A \implies B \iff \neg B \implies \neg A$[3].

Example 2.2. *Let X, Y be sets. Prove $X = X \setminus Y \implies X \cap Y = \emptyset$.*

Proof. Prove contrapositive: $X \cap Y \neq \emptyset \implies X \neq X \setminus Y$. $X \cap Y \neq \emptyset \implies \exists t \in X \cap Y \implies t \in X$ and $t \in Y$, thus $t \notin X \setminus Y$, but $t \in X$, so $X \neq X \setminus Y$. ■

2.4 Induction

Axiom 2.1 (Well-Ordering Principle). *Every $S \subseteq \mathbb{N}$, where $S \neq \emptyset$, has a minimal element, ie $\exists a \in S$ s.t. $\forall b \in S, a \leq b$.*

Theorem 2.1 (Principle of Induction). *Let $n_0 \in \mathbb{N}$. Say that for every $n \in \mathbb{Z}, n \geq n_0$, we are given a statement P_n. Assume*

(a) P_{n_0} is true

(b) if P_n is true, then P_{n+1} is true

then P_n is true for all $n \geq n_0$.

Proof (bwoc). Assume not.[4] Then, we define $S = \{n \in \mathbb{N} : n \geq n_0, P_n \text{ false}\}$. By the Well-Ordering Principle, there exists a minimal element $a \in S$. By definition, $a \geq n_0$, and as P_{n_0} is taken to be true, then $a > n_0$ since $n_0 \notin S$. Thus, $a - 1 \notin S$, as a is the minimal element of S, and therefore P_{a-1} is true. However, by (b), this implies P_a is also true, and thus $a \notin P$, contradicting our initial assumption. ■

2.5 Pigeonhole principle

Axiom 2.2. *If there are more pigeons than pigeonholes, then at least one pigeonhole must contain more than one pigeon.*[5]

[3] "I am hungry therefore I will eat" $\iff$ "I will *not* eat therefore I am *not* hungry." Notice too that B need not imply A ("I will eat therefore I am hungry"). If $A \implies B \iff B \implies A$, $A \equiv B$

[4] note that (a) and (b) of the Principle of Induction are still taken to be true; it is simply the conclusion that is assumed to be false.

[5] Alternatively, you can consider fractional pigeons (though a little gruesome); given $n+1$ pigeons and n holes, each hole will contain, on average, $1 + \frac{1}{n}$ pigeons.

Example 2.3. *Consider $n_1, \ldots, n_6 \in \mathbb{N}$. There exist at least two of these n's s.t. $n_i - n_j$ is evenly divisible by 5.*

Proof. Let us rewrite each n_i as $n_i = 5k_i + r_i$, where $k_i, r_i \in \mathbb{N}$, k_i is the quotient, and r_i is the residual. $r_i \in \{0, 1, 2, 3, 4\}$ (the only possible remainders when a number is divided by 5), and so there are 5 possible values of r_i, but 6 different n_i. Thus, two n_i must have the same r_i, and we can write:

$$\begin{aligned} n_i = 5k_i + r; n_j &= 5k_j + r \\ n_i - n_j &= (5k_i + r) - (5k_j + r) \\ &= 5(k_i - k_j) \end{aligned}$$

$(k_i - k_j) \in \mathbb{Z}$, and so $n_i - n_j$ is evenly divisible by 5. ■

3 Functions

3.1 Types of Functions

Definition 3.1 (Function). *Given 2 sets A, B, a* function *$f : A \to B$ is a rule such that $\forall a \in A, \exists! f(a) \in B$, where $\exists!$ denotes "there exists a unique".*

Definition 3.2 (Graph). *Given a function $f : A \to B$, a* graph *$\Gamma_f = \{(a, f(a)) : a \in A\} \subseteq A \times B$. We can say that, $\forall a \in A, \exists! b \in B$ such that $(a, b) \in \Gamma_f$.*

Example 3.1. *Consider the Cartesian plane, denoted $\mathbb{R}^2$. It is simply a graph Γ_f where $f : \mathbb{R} \to \mathbb{R}$ is the identity function, $f(x) = x$.*

Definition 3.3 (Injective). *A function is an* injection *iff $\forall a_1, a_2 \in A, f(a_1) = f(a_2) \implies a_1 = a_2$.*

Definition 3.4 (Surjective). *A function is a* surjection *iff $\forall b \in B, \exists a \in A$ such that $f(a) = b$. In other words, every element of B is mapped to by at least one element of A; you can pick any element in the range and it will have a preimage.*

Definition 3.5 (Bijective). *Both.*

Definition 3.6 (Fibre). *The fibre of some $y \in Y$ is $f^{-1}(y) = f^{-1}(y)$*

3.2 Cardinality

Definition 3.7 (Cardinality)**.** *The cardinality of a set A, denoted $|A|$, is the number of elements in A, if A is finite, or a more abstract notion of size if A is infinite.*

We say that two sets A, B have the same cardinality ($|A| = |B|$) if $\exists$ a bijection $f : A \to B$.[6]This necessitates the question, however: if two sets are not equal in cardinality, how do we compare their sizes?

We write

$$|A| \leq |B| \impliedby \exists f : A \to B \text{ where } f \text{ is } \textit{injective}$$

and

$$|A| \geq |B| \impliedby \exists f : A \to B \text{ where } f \text{ is } \textit{surjective.}$$[7]

Note that $|B| \leq |A|$ if either $A = \varnothing$ or, as above, $\exists f : B \to A$ surjective.

Definition 3.8 (Composition)**.** *Given two functions $f : A \to B$, $g : B \to C$, the* composition *is the function $g \circ f : A \to C$*

Proposition 3.1. *If $|A| = |B|$ and $|B| = |C|$ then $|A| = |C|$*

Proof. $\exists f : A \to B$ bijective, and $\exists g : B \to C$ bijective. We desire to show that $\exists h : A \to C$ that is bijective. We can write $h = g \circ f$, where $h(a) = g(f(a))$.

To show that h bijective:

- **injective:** Suppose $h(a_1) = h(a_2)$, then $g(f(a_1)) = g(f(a_2))$, and since g is injective, $f(a_1) = f(a_2)$. Since f is injective, $a_1 = a_2$, and thus h is injective.
- **surjective:** Let $c \in C$. Since g is surjective, $\exists b \in B$ such that $g(b) = c$. Since f is surjective, $\exists a \in A$ such that $f(a) = b$. Thus, $h(a) = g(f(a)) = g(b) = c$, and thus h is surjective.

Thus, h is bijective, and $|A| = |C|$. ■

Lemma 3.1. *If $g \circ f$ injective, f injective. If $g \circ f$ surjective, g surjective.*

Definition 3.9 (Image)**.** *The image of a function $f : A \to B$ is the set $Im(f) = \{f(a) : a \in A\}$, ie the set of all elements in B that are mapped to by f. Note that $Im(f) \subseteq B$, and $Im(f) = B$ if f is surjective.*

[6] Consider this in the finite case: a bijection indicates that all elements in the domain map uniquely to a single element in the range, and the range is completely "covered" sts by the function.

[7] Consider this intuitively; if your domain is smaller than your range, then you will "run out" of things to map from the domain to the range before you "run out" of things in the range, hence, you have a injection. Similarly, if your domain is larger than your range, then you will have "leftover" elements in the domain (that will map to "already mapped to" elements in the range), hence, you have a surjection.

Proposition 3.2. $|A| \leq |B| if |B| \geq |A|$

Proof. If $A = \varnothing$, $|B| \geq |A|$ clearly.

If $A \neq \varnothing$, we are given $\exists f : A \to B$ injective. Let us choose some $a_0 \in A$. We define $g : B \to A$ as

$$g(b) = \begin{cases} a_0 & b \notin \text{Im}(f) \\ a & b = f(a) \in \text{Im}(f)^{8} \end{cases}$$

Note that $g(f(a)) = g(b) = a$, so g is surjective. Thus, $|B| \geq |A|$. ■

Proposition 3.3. $|B| \geq |A|$ *if* $|A| \leq |B|$

Theorem 3.1 (Cantor-Bernstein Theorem). $|A| \leq |B|$ *and* $|B| \leq |A| \implies |A| = |B|$. [9]

Equivalently, if $\exists f : A \to B$ *injective and* $\exists g : B \to A$ *injective, then* $\exists h : A \to B$ *bijective.*

Proposition 3.4. *If* $|A_1| = |A_2|$ *and* $|B_1| = |B_2|$ *then* $|A_1 \times B_1| = |A_2 \times B_2|$.

Proof. The first two statements define bijections $f : A_1 \to A_2$ and $g : B_1 \to B_2$, and we desire to have $f \times g : A_1 \times B_1 \to A_2 \times B_2$. We define $f \times g(a_1, b_1) := (f(a_1), g(b_1))$. We must show that $f \times g$ is bijective. ■

Example 3.2. *Consider* A *as the set of all points in the unit circle centered at* $(0,0)$ *in* $\mathbb{R}^2$*, and* B *as the set of all points in the square of side length 2 centered at* $(0,0)$ *in* $\mathbb{R}^2$ *(ie, the circle is inscribed in the square). We wish to prove that* $|A| = |B|$.

Proof. Let $f : A \to B$, $f(x) = x$. f is injective, and thus $|A| \leq |B|$. Let $g : A \to B$, $g(x) = \begin{cases} 0; \sqrt{2}x \notin B \\ \sqrt{2}x; \sqrt{2}x \in B \end{cases}$. In simpler terms, consider this as multiplying points of A by $\sqrt{2}$; any point in this new "expanded" circle that lies within B maps to itself, and any that lies outside maps to 0. This is thus a surjection, and thus $|B| \leq |A|$. By the Cantor-Bernstein Theorem, $|A| = |B|$. ■

Proposition 3.5. $A = \{0, 1, 4, 9, \dots\}$. $|A| = |\mathbb{N}|$.

Proof. Define $f : \mathbb{N} \to A$, $f(n) = n^2$. This is clearly injective [10], and thus $|A| \leq |\mathbb{N}|$. ■

Definition 3.10 (Countable/enumerable). *A set* A *is* countable *if* $|A| = |\mathbb{N}|$*, or* A *is finite.*

If A *is finite of size* n, $\exists$ *a bijection* $f : \{0, 1, 2, \dots, n-1\} \to A$.

If A *is infinite,* $\exists$ *a bijection* $f : \mathbb{N} \to A$.

Proposition 3.6. $|\mathbb{N}| = |\mathbb{Z}|$

[8] Note that a is unique in A, as f is injective.

[9] It is often very difficult to define an arbitrary bijective function between two sets in order to prove their cardinality is equal. The Cantor-Bernstein Theorem allows us to prove that two sets have the same cardinality by proving that there exists an injection from A to B and an injection from B to A, which is typically far easier.

[10] Notice that f is only injective if we restrict the domain to $\mathbb{N}$; if we were to consider $\mathbb{Z}$, for instance, $f(-1) = f(1) = 1$.

Proof. We aim to find a bijection $f : \mathbb{Z} \to \mathbb{N}$, ie one that maps integers to natural numbers. Consider the function

$$f(x) = \begin{cases} 2x & x \geq 0 \\ -2x - 1 & x < 0 \end{cases}.$$

This function is an injection because if $f(x_1) = f(x_2)$, then $x_1 = x_2$ (positive case: $2x_1 = 2x_2 \implies x_1 = x_2$, negative case: $-2x_1 - 1 = -2x_2 - 1 \implies x_1 = x_2$, and $2x_1 \neq -2x_2 - 1$ for any integer). It is also a surjection (there is no natural number that cannot be mapped to by an integer). Thus, the function is a bijection and $|\mathbb{N}| = |\mathbb{Z}|$. [11] ■

Proposition 3.7. $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$

Remark 3.1. *It is possible to construct a bijective* $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$*; see assignment 1.*

Proof. Let $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$, $f(n) = (n, 0)$, clearly an injection ($\implies |\mathbb{N}| \leq |\mathbb{N} \times \mathbb{N}|$)[12]. The function $g(m, n) = 2^n 3^m$ is also injective, and thus $|\mathbb{N}| = |\mathbb{N} \times \mathbb{N}|$. ■

Corollary 3.1. $|\mathbb{Z}| = |\mathbb{Z} \times \mathbb{Z}|$

Proof. Consider $h : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$, a bijection[13], and $f : \mathbb{N} \to \mathbb{Z}$. Let $g = (f, f) : \mathbb{N} \times \mathbb{N} \to \mathbb{Z} \times \mathbb{Z}$. The composition $g \circ h \circ f^{-1} : \mathbb{Z} \to \mathbb{N} \to \mathbb{N} \times \mathbb{N} \to \mathbb{Z} \times \mathbb{Z}$ is also a bijection, and thus $|\mathbb{Z}| = |\mathbb{Z} \times \mathbb{Z}|$. ■

Example 3.3. *Show that* $|\mathbb{N}| = |\mathbb{Q}|$.

Proof. First, we find an injection $\mathbb{Q} \to \mathbb{N}$. Let $f : \mathbb{Q} \to \mathbb{Z} \times \mathbb{Z}$, $f(n) = (p, q)$ where $\frac{p}{q} = n$ (by definition of $\mathbb{Q}$). Using the same function definitions as in Corollary 3.1, the composition $h^{-1} \circ g^{-1} \circ f : \mathbb{Q} \to \mathbb{Z} \times \mathbb{Z} \to \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. This is a composition of injections, and is thus an injection itself, and thus $|\mathbb{Q}| \leq |\mathbb{N}|$. The identity function $1 : \mathbb{N} \to \mathbb{Q}, 1(n) = n$ is clearly an injection as well as all naturals are rationals, and thus $|\mathbb{N}| \leq |\mathbb{Q}|$. By the Cantor-Bernstein Theorem, $|\mathbb{N}| = |\mathbb{Q}|$. ■

Definition 3.11. *We say* $|A| < |B|$ *if* $|A| \leq |B|$ *but* $|A| \neq |B|$, *ie* $\exists f : A \to B$ *is injective, but no such bijective.*

Remark 3.2. *We denote an injective function as* $\mathbb{N} \hookrightarrow \mathbb{Z}$, *and a surjective function as* $\mathbb{Z} \twoheadrightarrow \mathbb{N}$. *We say that a particular element* n *maps to some other element* n' *by* $n \mapsto n'$

Theorem 3.2 (Cantor). $|\mathbb{N}| < |\mathbb{R}|$

Proof (Cantor's Diagonal Argument). We clearly have an injection $\mathbb{N} \hookrightarrow \mathbb{R}, n \mapsto n$, thus $|\mathbb{N}| \leq |\mathbb{R}|$.

[11] Note what would happen if f was defined as $-2x$ for $x < 0$; then, f would not be surjective (eg, $f(-1) = 2 = f(1)$.)

[12] Note that this function is *not* surjective!

[13] Which must exist by the proof of the previous proposition.

Now, suppose $|\mathbb{N}| = |\mathbb{R}|$. Then, we can enumerate the real numbers as $a_0, a_1, \ldots$ with signs ϵ_i. We denote the decimal expansion of each number as[14]

$$\begin{aligned} a_0 &= \epsilon_0 0.a_{00}a_{01}a_{02}\ldots \\ a_1 &= \epsilon_1 0.a_{10}a_{11}a_{12}\ldots \\ a_2 &= \epsilon_2 0.a_{20}a_{21}a_{22}\ldots \\ &\vdots \end{aligned}$$

Consider the number $0.e_0e_1e_2\ldots$, where $e_i = \begin{cases} 3 & a_{ii} \neq 3 \\ 4 & a_{ii} = 3 \end{cases}$. This number is different than any given a_i at the $i+1$-th decimal place, and is thus not in the enumeration, contradicting our initial assumption. ■

Remark 3.3 (Continuum Hypothesis)**.** *Cantor claimed that there's no set $|A|$ such that $|\mathbb{N}| < |A| < |\mathbb{R}|$. It has been proven today that this is "undecidable".*

Definition 3.12 (Algebra on Cardinalities)**.** *If α, β are cardinalities $\alpha = |A|, \beta = |B|$, Cantor defined:*

$$\begin{aligned} \alpha + \beta &= |A \sqcup B| \textit{ (disjoint union)} \\ \alpha \cdot \beta &= |A \times B| \\ \alpha^\beta &= |B^A| \textit{ (set of all functions from } A \textit{ to } B\textit{)} \end{aligned}$$

4 Relations

4.1 Definitions

Definition 4.1 (Relation)**.** *A* relation *on a set A is a subset $S \subseteq A \times A (= \{(x, y) : x, y \in A\})$.*

We say that x is related to *y if $(x, y) \in S$, where we denote $x \sim y$.*

Conversely, if we are given $x \sim y$, we can define an $S = \{(x, y) : x \sim y\}$.

Example 4.1. *Following are examples of relations on A.*

1) *Let $S = A \times A$; any $x \sim$ any y because $(x, y) \in S$ for all (x, y).*

2) *Let $S = \varnothing$; no $x \sim$ any y (even to itself).*

3) *$S =$ diag. $= \{(a, a) : a \in A\}$; $x \sim x \forall x$, but $x \nsim y$ if $y \neq x$.*

4) *$A = [0, 1] (\in \mathbb{R})$. Say $x \sim y$ if $x \leq y$. Thus, $S = \{(x, y) : x \leq y\}$ (the diagonal, and everything above).*

5) *$A = \mathbb{Z}$, $x \sim y$ if $5|(x - y)$, ie x and y have same residue mod 5.*[15]

[14] We make the clarification that, despite the fact that $1.000\cdots = 0.999\ldots$, we will take the "infinite zeroes" interpretation, and thus every real number has a unique decimal expansion. This is an important, if subtle, distinction.

Definition 4.2 (Reflexive). *A relation is* reflexive *if for any $x \in A$, $x \sim x$.*

This includes examples 1), 2) (iff A is empty), 3), 4), and 5) above.

Definition 4.3 (Symmetric). *A relation is* symmetric *if $x \sim y \implies y \sim x$.*

This includes 1), 2), 3), and 5) above.

Definition 4.4 (Transitive). *A relation is* transitive *if $x \sim y$ and $y \sim z$ implies $x \sim z$.*

This includes 1), 2), 3), 4), and 5) above.

4.2 Orders, Equivalence Relations and Classes, Partitions

Definition 4.5 (Partial Order). *A* partial order *on a set A is a relation $x \sim y$ s.t.*

1. *$x \sim x$ (reflexive)*
2. *if $x \sim y$* and *$y \sim x$, $x = y$ (antisymmetric)*
3. *$x \sim y$* and *$y \sim z \implies x \sim z$ (transitive)*

It is common to use $\leq$ in place of $\sim$ for partial orders.

We call a set on which a partial order exists a partially ordered set *(poset).*

This is called partial, as it is possible that for some $x, y \in A$ we have $x \nsim y$ and $y \nsim x$, ie x, y are not comparable. A partial order is called linear/total *if for every $x, y \in A$, either $x \leq y$ or $y \leq x$, eg., $A = [0, 1], \mathbb{R}, \mathbb{Z}, \ldots$, with $x \leq y$. Consider the above examples:*

1) *is not total, if A has at least two element, because $\exists x \neq y$ but both $x \sim y$ and $y \sim x$, and thus not antisymmetric.*

3) *yes*

5) *no, as this is symmetric, since $5|(x - y) \implies 5|(y - x)$, and thus $x \sim y, y \sim x \cancel{\implies} y = x$*

Example 4.2. *Let[16] $A = \mathbb{N}_+ = \{1, 2, 3, 4 \ldots\}$, and define $a \sim b$ if $a|b$. We verify:*

- *$a \sim a$ (since $a|a$)*
- *$a \sim b, b \sim a \implies a = b$, since in $\mathbb{N}_+$, $a|b \implies a \leq b$, and we thus have $a \leq b$ and $b \leq a$, and thus $a = b$.*
- *suppose $a \sim b$ and $b \sim c$, then $a|b$ and $b|c$. We can write $b = a \cdot m$ and $c = b \cdot n$ for $n, m \in \mathbb{N}$. This means that $c = bn = amn = a(mn)$, which means that $a|c$, so $a \sim c$.*

Thus, A is a poset. Note that this is not a linear order, as $2 \nsim 3$, and $3 \nsim 2$ (not all a, b are comparable).

[15] Where $a|b$ denotes that b divides a.

Definition 4.6 (Equivalence Relation)**.** *We aim to, abstractly, define some $\sim$ such that if $x \sim x, x \sim y$, then $y \sim x$, and if $x \sim y, y \sim z$, then $x \sim z$.*

Specifically, an equivalence relation $\sim$ on the set A is a relation $x \sim y$ s.t. it is

- *reflexive;*
- *symmetric;*
- *transitive.*[17]

Example 4.3. 1. *Let $n \geq 1$ be an integer. A* permutation *σ of n elements is a bijection $\sigma : \{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$. Their number is $n!$, ie there are $n!$ permutations of n elements. The collection of all permutations of n elements is denoted S_n, which we call the "symmetric group" on n elements. We aim to define an equivalence relation on S_n.*

Let us define $\sigma \sim \tau$ if $\sigma(1) = \tau(1)$. We verify that this is an equivalence relation:

(a) *$\sigma \sim \sigma, \sigma(1) = \sigma(1)$, so yes*

(b) *$\sigma \sim \tau$ means $\sigma(1) = \tau(1)$, so yes*

(c) *$\sigma \sim \tau, \tau \sim \rho, \sigma(1) = \tau(1), \tau(1) = \rho(1)$, so $\sigma(1) = \rho(1)$, hence $\sigma \sim \rho$, so yes.*

Thus, $\sim$ is an equivalence relation on S_n.

Example 4.4. *Define a relation on $\mathbb{Z}$ by saying that $x \sim y$ if $x - y$ even, ie $2 | (x - y)$. This is reflexive, as $2 | (x - x) = 0, x \sim x$, symmetric, since $(y - x) = -(x - y)$, and transitive $x - z = \underbrace{(x - y)}_{\text{even}} + \underbrace{(y - z)}_{\text{even}} \implies x \sim z$.*

Example 4.5. *We say two sets $A \sim B$ if $|A| = |B|$. $1_A = Id : A \to A, a \mapsto a$ shows $A \sim A$. $A \sim B \implies \exists f : A \to B$ bijective, then $f^{-1} : B \to A$ also bijective so $B \sim A$. If $A \sim B, B \sim A$ then $A \sim C$ (since $|A| = |B|, |B| = |C| \implies |A| = |C|$ as proved earlier).*

Definition 4.7 (Disjoint Union)**.** *Let S be a set, and $S_i, i \in I, \subseteq S$. S is the* disjoint union *of the S_i's if $S = \cap_{i \in I} S_i$, and for any $i \neq j$, $S_i \cap S_j = \varnothing$*[18]*; we denote $S = \amalg_{i \in I} S_i$. We can say that $\{S_i\}$ for a* partition *of S.*

Example 4.6. *Let $S = \{1, 2\}$. Partitions are $\{1, 2\}$, and $\{1\}, \{2\}$.*

Let $S = \{1, 2, 3\}$. Partitions are $\{1, 2, 3\}, \{1\}, \{2\}, \{3\}, \dots$

Definition 4.8 (Equivalence Class)**.** *Given an equivalence relation $\sim$ of A and some $x \in A$, the* equivalence class *of x is $[x] = \{y \in A : x \sim y\} \subseteq S$.*

[16] Try this with integers, see where it fails

[17] Note that, generally, equivalence and order relations are very different.

[18] ie, no S_i's share elements; think of "partitioning" S such that no subsets overlap.

Theorem 4.1. *The following theorems are related to equivalence classes:*

(1) the equivalence classes of A form a partition of A;

(2) conversely, any partition of A defines an equivalence relation on A given by the partition.

Lemma 4.1. *Let X be an equivalence class; $a \in X$, then $X = [a]$.*

Proof of Lemma 4.1. If X is an equivalence class, $X = [x]$ for some $x \in A$, by definition. Let $a \in X$. If $b \in [a]$ then $b \sim a$ and as $a \in [x]$ then $a \sim x \implies b \sim x \implies b \in [x] \implies [a] \subseteq [x]$.

Otoh, $a \sim x \implies x \in [a]$, so $[x] \subseteq [a]$, and thus $[x] = [a]$. ■

Proof of Theorem 4.1. We prove (1), (2) individually.

(1) We aim to show that if the equivalence classes are $\{X_i\}_{i \in I}$ then $A = \amalg_{i \in I} X_i$. We say the following:

1. Every $a \in A$ is in some equivalence class ($a \in [a]$).
2. Two different equivalence classes are disjoint $\iff$ if X, Y equiv. classes s.t. $X \cap Y \neq \varnothing$ then $X = Y$.[19]

Let $a \in X \cap Y \overset{\text{lemma}}{\implies} [a] = X, [a] = Y \implies X = Y$.

Here, consider the examples above;

- Example 4.3; S_n: there are n equiv classes $X_i = \{\sigma \in S_n : \sigma(1) = i\}$. $S_n = X_1 \sqcup X_2 \sqcup \ldots X_n$. $\sigma \in S_n$ and $\sigma(1) = i$, then $\sigma \in X_i$.
- Example 4.4; $\mathbb{Z}$: two equiv. classes; $X =$ even integers $= [0]$, $Y =$ odd integers $= [1]$, so $\mathbb{Z} =$ even $\sqcup$ odd
- Example 4.5; sets: an equivalence *is* a cardinality. $n := [\{1, 2, \ldots n\}] =$ all sets with n elements. Similarly, we often write that $\aleph_0 := [\mathbb{N}] =$ inf. countable sets = sets un bijection with $\mathbb{N}$, and $2^{\aleph_0} := [\mathbb{R}]$.

(2) We are given a partition $A = \amalg_{i \in I} X_i$. We say $x \sim y$ if $\exists i \in I$ s.t. x and y belong to X_i (noting that such an i is unique if it exists by definition of a partition).

- $x \sim x$, clearly, since $x \in X_i \implies x \in X_i$
- $x \sim y \implies y \sim x$, by similar logic
- $x \sim y, y \sim z$ means that x and y in some same X_i, and y and z in some same X_j. So, $y \in X_i \cap X_j$, but we are working with a partition so X_i and X_j are disjoint and so this intersection is either $\varnothing$, or the sets are equal; since we know it is not empty, $X_i = X_j$, and so $x \sim z$.

Thus, $\sim$ is an equivalence relation.[20] ■

Example 4.7. *Let A = students in this class. $x \sim y$ if x, y have the same birthday. The equivalence classes in this case are the dates s.t. $\exists$ some student with that birthday.*

Definition 4.9 (Complete set of representatives). *If is an equiv. relation on A, a subset $\{a_i : i \in I\} \subseteq A$ is called a* complete set of representatives *if the equivalence classes are $[a_i], i \in I$ with no repetitions.*

You find such a subset by choosing from every equiv class one element.Considering our examples:

- *For Example 4.3, $S_n = X_1 \sqcup \ldots X_n$, $X_i = \{\sigma : \sigma(1) = i\}$. We define*

$$\sigma_i(j) = \begin{cases} i & j = 1 \\ 1 & j = i \\ j & \textit{otherwise} \end{cases} = [\sigma_i]$$

  (switch i, j and leave all others intact). $\{\sigma_1, \ldots, \sigma_n\}$ are a complete set of representatives.

- *For Example 4.4 (even/odd in $\mathbb{Z}$), a complete set of reps could be $\{0, 1\}$, ie $\mathbb{Z} = [0] \sqcup [1]$.*

5 Number Systems

5.1 Complex Numbers

Definition 5.1 (Complex Numbers). $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$. *Equivalently, we can consider complex numbers as the points $(a, b) \in \mathbb{R}^2$.*[21]

Given some $z = a + bi$, we can write Re$(z) = a$, Im$(z) = b$.

Definition 5.2 (Algebra on Complex Numbers). *Given $z_i = x_i + y_i i$, we define:*

- Addition*: $z_1 + z_2 = (x_1 + x_2) + (y_1 + y_2)i$. This is associative and commutative.*
- Multiplication*: $z_1 z_2 = (x_1 x_2 - y_1 y_2) + (x_1 y_2 + x_2 y_1)i$*
- Inverse*: $z \neq 0$, $\frac{1}{z} := \frac{\overline{z}}{|z|^2}$, noting that $z \cdot \frac{1}{z} = z \cdot \frac{\overline{z}}{|z|^2} = 1$*

Definition 5.3 (Complex Conjugate). *Given $z = a + bi$, the* complex conjugate *of z is $\overline{z} = a - bi$.*

[20] Contrapositive...

[20] This whole proof/theorem can sound pretty confusing. Abstractly, and non-rigorously, consider this: we define some "notion" of equivalence. Intuitively, if a set of items in, say, A, are equivalent, then they shouldn't be equivalent to any other items outside of that set (by our particular definition of equivalence). Thus, no "subsetting" of A into equivalence classes will cause any subset to overlap; thus, we have a partition. This works in reverse through similar logic, where we even more concretely say that the very act of begin in the same partitioning of A is to be equivalent.

[21] We can define the function $f : \mathbb{C} \to \mathbb{R}^2, f(a + bi) = (a, b)$, a bijection.

Lemma 5.1. *The following hold for complex conjugates:*[22]

(a) $\overline{\overline{z}} = z$.

(b) $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}, \overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$.

(c) *Re* $(z) = \frac{z+\overline{z}}{2}$, *Im* $(z)\, i = \frac{z-\overline{z}}{2}$.

(d) *Given* $|z| = \sqrt{a^2 + b^2}$,

   (i) $|z|^2 = z \cdot \overline{z}$

   (ii) $|z_1 + z_2| \leq |z_1| + |z_2|$

   (iii) $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$

5.2 Fundamental Theorem of Algebra, Etc

Theorem 5.1 (Fundamental Theorem of Algebra). *Any polynomial* $a_n x^n + \cdots + a_1 x + a_0$ *for* $a_i \in \mathbb{C}, n > 0, a_n \neq 0$, *has a root in* $\mathbb{C}$.

Example 5.1 (Roots of Unity). *Let* $n \geq 1, n \in \mathbb{Z}$. $x^n = 1$ *has* n *solutions in* $\mathbb{C}$, *called the roots of unity of order* n. *They are given as* $(1, \frac{2\pi k}{n}), k = 0, 1, 2, \ldots, n-1$ *in polar notation.*

[22] (a), (b), and (c) are simply algebraic rearrangements of two complex numbers. (d.i) and (d.iii) follow from similar arguments, and finally (ii) is the triangle inequality restated in terms of complex numbers.

Theorem 5.2. *Let $f(x) = a_nx^n + \cdots + a_1x + a_0$ be a complex polynomial of degree n. Then, there are complex numbers $z_1, \ldots .z_n$ s.t.*

$$f(x) = a_n \prod_{i=1}^{n} (x - z_i) \qquad (i)$$

each (ii) $f(z_j) = 0 \forall j = 1, \ldots, n$, and (iii) $f(\lambda) = 0 \implies \lambda = z_j$ for some j.[23]

Proof (by induction). If $n = 1$, $f(x) = a_1x + a_0 = a_1\left(x - \frac{-a_0}{a_1}\right) = a_1(x - z_1)$. Clearly, $f(z_1) = 0$.

Assume that true for polynomials of degree $\leq n$ and prove for $n+1$; let f be a polynomial of degree $n+1$, $f(x) = a_{n+1} + x^{n+1} + \cdots$. Let z_{n+1} be a root of $f : f(z_{n+1}) = 0$. Such exists by the Fund'l Thm. We introduce the following lemma:

Lemma 5.2. *Let g be a polynomial with complex coefficients. Let $\lambda \in \mathbb{C}$; then we can write $g(x) = (x - \lambda)h(x) + r, r \in \mathbb{C}, h$ a polynomial with complex coefficients as well.*

Proof of Sub-Lemma. By induction; we can write $g(x) = a_nx^n + \cdots a_1x + a_0$. If $\deg(g) = 0$, then $g = a_0 \implies h(x) = 0, a_0 = r$.

Assume this is true for degrees $\leq n$,and that g has degree $\leq n+1$.

$$g(x) = (x - \lambda)a_{n+1}x^n + b(x),$$

where $b(x) = g(x) - (x - \lambda)a_{n+1}x^n = a_n'x^n + a_{n-1}'x^{n-1} + \cdots$, for some $a_n', \ldots, a_0' \in \mathbb{C}$. We can apply induction to $b(x)$ (that has $\deg \leq n$); $b(x) = (x - \lambda)h_1(x) + r$, so

$$g(x) = (x - \lambda)\underbrace{(a_{n+1}x^n + h_1(x))}_{h(x)} + r,$$

as desired. ■

Now, we write our $f(x)$ as

$$f(x) = (x - z_{n+1})h(x) + r,$$

using the lemma. Then,

$$\begin{aligned} 0 = f(z_{n+1}) &= (z_{n+1} - z_{n+1})h(z_{n+1}) + r \\ &= 0 + r + 0 \implies r = 0, \end{aligned}$$

so

$$f(x) = (x - z_{n+1})h(x).$$

[23] Proof sketch: we prove by induction. First, we prove the base case of polynomials of deg $= 1$, then we assume it holds for deg $\leq n$. We then prove a separate lemma (also by induction) that allows us to rewrite our polynomial as the product of some $(x - \lambda)$ factor, another polynomial, and some residual. We then rewrite our original polynomial as the product of some linear term and another polynomial, plus some residual, then show that this residual is 0, and thus show that our polynomial of degree $n+1$ is simply the product of some linear term and a polynomial of degree n, the inductive assumption, and thus the general statement is true.
The "sub"-claims follow naturally.

Comparing the highest terms:

$$a_{n+1}x^{n+1} + \dots = (x - z_{n+1})(*x^n + \dots)$$
$$\implies \text{leading coefficient of } h(x) \text{ also } a_{n+1}.$$

By induction,

$$h(x) = \underbrace{a_{n+1}}_{\text{lead coef of } h} \cdot \prod_{i=1}^{n}(x - z_i)$$
$$\implies f(x) = a_{n+1}\prod_{i=1}^{n+1}(x - z_i) \qquad (i) \text{ holds}$$

Further:

- (ii): $f(z_j) = a_{n+1}\prod_{i=1}^{n+1}(z_j - z_i) = 0$ when $i = j$.
- (iii): if $f(\lambda) = 0$, then $a_{n+1}\prod_{i=1}^{n+1}(\lambda - z_i) = 0$. But if a product of two complex numbers is 0, then one of them is 0. $a_{n+1} \neq 0$, so some $\lambda - z_i = 0$, ie $\lambda = z_i$ for some i[24]

■

Definition 5.4 (Complex Exponential). *The complex exponential,* $e^z = 1 + \frac{z}{1} + \frac{z^2}{2!} + \dots$ *can be Taylor expanded and we have that*

$$e^{i\theta} = \cos\theta + i\sin\theta.$$

Example 5.2. *If* $z = e^{x+yi} = e^x \cdot e^{yi} = e^x(\cos y + i\sin y)$*, then* $z = (e^x, y)$ *in polars.*

We can apply this idea to prove some trigonometric formulas. Consider $e^{2i\theta}$*;*

$$e^{2i\theta} = (\cos\theta + i\sin\theta)^2 = \underbrace{\cos^2\theta - \sin^2\theta}_{Re} + \underbrace{2\sin\theta\cos\theta}_{Im} i$$
$$e^{2i\theta} = \underbrace{\cos(2\theta)}_{Re} + i\underbrace{\sin(2\theta)}_{Im}$$
$$\implies \cos(2\theta) = \cos^2\theta - \sin^2\theta$$
$$\implies \sin(2\theta) = 2\sin\theta\cos\theta$$

[24] This claim relies on the claim that $s_1 \cdot s_2 = 0 \iff s_1$ or $s_2 = 0$ for $s_1, s_2 \in \mathbb{C}$. This is fairly straightforward to prove, and can be extended to any number of complex numbers, ie $\prod_{i=1}^{n} s_i = 0 \iff$ some $s_i = 0$

6 Rings

6.1 Definitions

Definition 6.1 (Ring). *A ring R is a set with two operations*[25]

- Addition: $R \times R \xrightarrow{+} R, \quad (a,b) \mapsto a + b$
- Multiplication: $R \times R \xrightarrow{\cdot} R, \quad (a,b) \mapsto a \cdot b$

The following hold:

1. *(+ is commutative)* $a + b = b + a, \forall a, b \in R$.
2. *(+ is associative)* $a + (b + c) = (a + b) + c, \forall a, b, c \in R$.
3. *(0)* $\exists$ *a zero element, 0, s.t.* $0 + a = a + 0 = a, \forall a \in R$.
4. *(negative)* $\forall a \in R, \exists b \in R$ *s.t* $a + b = 0$.
5. *($\cdot$ associative)* $a(bc) = (ab)c, \forall a, b, c \in R$.
6. *(1, multiplicative identity)* $\exists 1 \in R$ *s.t.* $1 \cdot a = a \cdot 1 = a, \forall a \in R$.[26]
7. *(distributive)* $\forall a, b, c \in R$, $a(b + c) = ab + ac$

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{R}[i] := \{a + b_i : a, b \in \mathbb{Z}\}, M_2(\mathbb{Z}) := \{\begin{matrix} a & b \\ c & d \end{matrix} : a, b, c, d \in \mathbb{Z}\}, \ldots$ *are all examples of rings.*

Remark 6.1. *We de note require multiplication to be commutative; if it is, we call R a* ***commutative ring*** *(eg $M_2(\mathbb{Z}), M_2(\mathbb{R})$ are not commutative).*

We also do not require inverse for multiplication (eg 2 doesn't have an inverse in $\mathbb{Z}$).

Definition 6.2 (Field). *A* commutative, *non-zero, ring R s.t. $\forall x \in R$ and $x \neq 0$ ($\iff 1 \neq 0$ in R, ie R is not a zero ring), $\exists y \in R$ s.t. $xy = yx = 1$ is a* field.

Fields include $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}[i]$

Definition 6.3 (Zero Ring). $\{0\}$ *with* $0 + 0 = 0, 0 \cdot 0 = 0$, *where* $1 = 0$ *(identity element is 0).*

Example 6.1. *Show that $\mathbb{Q}[i]$ is a field.*

If $x \in \mathbb{Q}[i], x = a + bi \neq 0$ then

$$\frac{1}{a + bi} = \frac{a - bi}{(a + bi)(a - bi)} = \underbrace{\frac{a}{a^2 + b^2}}_{\in \mathbb{Q}} - \underbrace{\frac{b}{a^2 + b^2}}_{\in \mathbb{Q}} i \in \mathbb{Q}[i],$$

and thus $\mathbb{Q}[i]$ has multiplicative inverses in $\mathbb{Q}[i]$.

[26] Though not always explicitly stated, it is often specified that rings are *closed* under addition/multiplication; $a, b \in R \implies a + b$ and $a \cdot b \in R$.

[26] Some texts (Hungerford) do not require the multiplicative identity to exist in a ring; those with this property are called "rings with identity". In general, these are all relatively arbitrary conventions - they are defined as such to make other operations/observations clearer; they are not steadfast, natural definitions.

Corollary 6.1. *Note the following consequences of the above axioms:*

1. 0 *is unique; if* $x \in R$ *has the property that* $x + a = a + x = a \forall a \in R$*, then* $x = 0$*.*

2. 1 *is unique; if* $x \in R$ *has the property that* $x \cdot a = a \cdot x = a \forall a \in R$*, then* $x = 1$*.*

3. *The element* b *s.t.* $a + b = b + a = 0$ *is uniquely determined by* a*; if* $x \in R$ *and* $x + a = a + x = 0$*, then* $x = b$*. We denote such* b *as* $-a$*, ie*

$$-a + a = a + (-a) = a - a = 0.$$

4. $-(-a) = a$*.*

5. $-(x + y) = -x - y$*.*

6. $x \cdot 0 = 0 \cdot x = 0 \forall x \in R$*.*

Definition 6.4 (Subring)**.** *Let* R *be a ring. A subset* $S \subseteq R$ *is a* subring *if*

1. $0, 1 \in S$*.*

2. $x, y \in S \implies x + y, -x, x \cdot y \in S$*.*

Then, S *is a ring itself.*

$\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ *are subrings;* $\mathbb{Z} \subseteq \mathbb{Z}[i] \subseteq \mathbb{Q}[i] \subseteq \mathbb{C}$ *are subrings;* $M_2(\mathbb{Z}) \subseteq M_2(\mathbb{R})$ *are subrings.*

II. Arithmetic in the Integers

Math $\equiv$ Poetry

7 Division

7.1 With Residue

Theorem 7.1. *Let $a, b \in \mathbb{Z}$ with $b \neq 0$. There exist unique integers q (quotient) and r s.t.*

$$a = q \cdot b + r, 0 \leq r < |b|.$$

Proof. Assume $b > 0$ (similar proof applies for $b < 0$). Consider the set $S = \{a - bx : x \in \mathbb{Z}, a - bx \geq 0\}$. Note that $S \neq \varnothing$. If $a \geq 0$, take $x = 0$. If $a < 0$, take $x = a$ to get $a - bx = a - ba = a(1 - b) \geq 0$.
Thus, S has a minimal element; let $r = \min(S)$. Because $r \in S, r \geq 0$, and

$$r = a - bq \text{ some } q \in \mathbb{Z} \implies a = bq - r.$$

Here, we claim $r < b$. If $r \geq b$, then $0 \leq r - b = a - b(q + 1) \in S$, contradicting the minimality of r. Thus, $0 \leq r < b$.
We wish to show that q, r are unique, meaning that if $a = bq' + r', q' \in \mathbb{Z}, 0 \leq r < b \implies q = q', r = r'$.
If $q = q'$, then $r = a - bq = a - bq' = r'$✓.
Otherwise, wlog, say $q > q'$. We then have

$$\begin{aligned} 0 = a - a &= (bq + r) - (bq' + r') \\ &= b(q - q') + (r - r') \\ &\implies r' = r + b(q - q') \geq b, \perp (0 \leq r' < |b|) \end{aligned}$$

■

7.2 Without Residue

Definition 7.1. *Let $a, b \in \mathbb{Z}$. We say a divides b, $a|b$ if $b = a \cdot c$, some $c \in \mathbb{Z}$ (If $a \neq 0$, this is the case $\iff$ the residue of dividing b by a is 0).*

Lemma 7.1 (Properties of Division).

1. *0 is divisible by any integer a*
2. *0 only divides 0*
3. *$a|b \implies a|(-b)$*
4. *$a|b$ and $a|d \implies a|(b \pm d)$*
5. *$a|b \implies a|bd \forall d$*
6. *$a|b$ and $b|a \implies a = \pm b$*

Proof.

1. $0 = a \cdot 0 \forall a \checkmark$
2. $0|b$, then $b = 0 \cdot c$ some $c \implies b = 0 \quad \checkmark$
3. $b = ac \implies -b = a \cdot (-c) \quad \checkmark$
4. $b = a \cdot c_1$, $d = a \cdot c_2$. $b \pm d = a(c_1 \pm c_2) \in \mathbb{Z} \quad \checkmark$
5. $b = ac$, so $bd = a \cdot (cd) \quad \checkmark$
6. $a|b \implies b = a \cdot c, b|a \implies a = b \cdot d$. If either $a = 0$ or $b = 0$, both are 0, so $a = \pm b$. Assume $a \neq 0, b \neq 0$. Then, we have that $a = bd = acd \overset{a \neq 0}{\implies} cd = 1$. Either, $c = d = 1 \implies a = b$, or $c = d = -1 \implies a = -b \quad \checkmark$

■

Example 7.1. *Which integers could divide both n and $n^3 + n + 1$?*

Suppose d does. then $d|n$ and $d|(n^3 + n + 1)$, then $d|n^3 \implies d|(n^3 + n) \implies d|((n^3 + n + 1) - (n^3 + n))$, and so $d|1$ so $d = \pm 1$.

7.3 Greatest Common Divisor (gcd)

Definition 7.2 (GCD). *Let a, b be integers, not both 0. The $\gcd$ of a, b denoted $\gcd(a, b)$ is the greatest positive number divided both a and b.*

Remark 7.1. *Note that if both a, b are not 0, then $d = \gcd(a, b) \leq \min\{|a|, |b|\}$ because if $d|a$ then $a = d \cdot c \implies |a| = |d| \cdot |c| \implies |d| = d \leq |a|$.*
Similarly, $|d| \leq |b|$.

Theorem 7.2. *Let $a, b \in \mathbb{Z}$, not both 0. Let $d = \gcd(a, b)$. Then,*

1. *$\exists u, v \in \mathbb{Z}$ s.t. $d = ua + vb$;*
2. *d is the minimal positive integer of the form $ua + vb$, $u, v \in \mathbb{Z}$;*
3. *every common divisor of a, b divides d.*

Proof. Let $S = \{ma + nb : m, n \in \mathbb{Z}, ma + nb > 0\}$. $S \neq \varnothing$ because $a \cdot a + b \cdot b = a^2 + b^2 > 0$, so $a^2 + b^2 \in S$.
Let $D = \min(S)$, so $D = ua + vb, u, v \in \mathbb{Z}$. We claim that this D equals $d = \gcd(a, b)$.
We claim first that $D|a$. We can write

$$\begin{aligned} a &= D \cdot q + r, 0 \leq r < D, \\ r &= a - Dq = a - (ua + vb)q \\ &= a(1 - uq) + b(-vq) \\ &\implies r > 0 \implies r \in S, \text{ contradicts minimality of } D \end{aligned}$$

Thus, D divides both a and b, and so $D \leq d$ (any common divisor is leq gcd).
Let e be any common divisor of a, b. We have

$$e|a \implies e|ua \quad \text{and} \quad e|b, \implies e|vb \implies e|(ua + vb) = D.$$

In particular, $d|D \implies d \leq D$. It follows that $D = d$. ■

Example 7.2. $\gcd(7611, 592) = 1$.
One can write $1 = 195 \times 7611 - 2507 \times 592$. *How do we know? Mathematica.*

7.4 Euclidean Algorithm

Remark 7.2. $\gcd(-a, b) = \gcd(a, b) = \gcd(a, -b) = \cdots$

Theorem 7.3 (Euclidean Algorithm)**.** *Let a, b be positive integers $a \geq b$.*

If $b|a$, then $\gcd(a, b) = b$.

Else, perform the following:

$$\begin{aligned}
a &= b \cdot q_0 + r_0, \quad 0 < r_0 < b \\
b &= r_0 \cdot q_1 + r_1, \quad 0 < r_1 < r_0 \\
r_0 &= r_1 \cdot q_2 + r_2 \\
\vdots &\quad \vdots \\
r_{t-2} &= r_{t-1} \cdot q_t + r_t, \quad 0 < r_t < r_{t-1} \\
r_{t-1} &= r_t \cdot q_{t+1} + \underbrace{0}_{r_{t+1}}
\end{aligned}$$

Because the residues are non-negative decreasing integers, the process must stop; there is a first t s.t. $r_{t+1} = 0$. Then, $\gcd(a, b) = r_t$, the last non-zero residue.[27]

Proof. We first prove by induction that for all $0 \leq i \leq t+1$, r_t divides both r_{t-i} and r_{t-i-1}. ($\implies r_t|r_{-1} = b, r_t|r_{-2} = a$.)

(1) $i = 0$, then $r_t|r_t$ and $r_t|r_{t-1}$ (as $r_{t-1} = r_t \cdot q_{t+1}$)

(2) Suppose $r_t|r_{t-i}$ and $r_t|r_{t-i-1}$ for some $0 \leq i < t+1$. We have that

$$r_{t-i-2} = r_{t-i-1} \cdot q_{t-i} + r_{t-i}$$

We then have that

$$r_t|(r_{t-i} + r_{t-i-1}q_{t-i}) = r_{t-i-2},$$

so $r_t|\underbrace{r_{t-i-1}}_{r_{t-(i+1)}}$ and $r_t|\underbrace{r_{t-i-2}}_{r_{t-(i+1)-1}}$. Then, $r_t|\gcd(a, b)$.

Next we show that if $e|a$ and $e|b$ then $r|r_t$ ($\implies \gcd(a, b)|r_t$, then we would have $r_t = \gcd(a, b)$). We prove by induction on $0 \leq i \leq t+1$ that $e|r_{i-2}$ and $e|r_{i-1}$.

(1) $i = 0$, then $e|r_{-2} = a$ and $e|r_{-1} = b$, base case holds

(2) Suppose $e|r_{i-2}$ and $e|r_{i-1}$ for some $i < t+1$. We have that

$$r_{i-2} = r_{i-1} \cdot q_i + r_i, \quad e|(r_{i-2} - r_{i-1} \cdot q_i) = r_i.$$

So,

$$e|\underbrace{r_i}_{r_{(i+1)-2}} \quad \text{and} \quad e|\underbrace{r_i}_{r_{(i+1)-1}}$$

[27] Sketch: we show the equivalence by proving that they each divide each other, and are thus equal by Lemma 7.1. This is done by induction on the residuals dividing "each other", and working "backwards" essentially, then by induction on an arbitrary element dividing the residuals to show that it must then divide the gcd.

■

Remark 7.3 (Extended Euclidean Algorithm). *After completing the algorithm, one can then "work backwards" to write any $d = \gcd(a, b)$ as $d = ua + vb$.*
Start by writing $d = r_{t-2} - r_{t-1} \cdot q_t$; then, substitute in preceding residuals, simplifying along the way (but making sure to leave the quotients *from each substitution, as these are what you will substitute in the next step), and continue until you have the desired form. Consider the following example:*

Example 7.3. $a = 48, b = 27, d = \gcd 48, 27 = ?$

$$\begin{aligned}
48 &= 27 \cdot 1 + 21 \\
27 &= 21 \cdot 1 + 6 \\
21 &= 6 \cdot 3 + 3 \\
6 &= 3 \cdot 2 + 0 \\
&\implies \gcd(48, 27) = 3 \\
&\implies 3 = 21 - 6 \cdot 3 \\
&= 21 - (27 - 21)3 \\
&= 21 \cdot 4 - 27 \cdot 3 \\
&= (48 - 27) \cdot 4 - 27 \cdot 3 \\
&= 48 \cdot 4 - 7 \cdot 27
\end{aligned}$$

7.5 Primes

Definition 7.3 (Prime). *An integer $n \neq 0, 1, -1$ is called prime if its only divisors are $\pm 1, \pm n$.*
A positive integer n is prime iff its only positive divisors are $1, n$.

Remark 7.4. *The goal of this section is to prove Theorem 7.5, of unique prime factorization; we then extend it to the rationals. We introduce a number of lemmas/auxiliary results regarding primes to build up to the proof.*

Lemma 7.2. *Every natural number $n > 1$ is a product of prime numbers.*

Proof. We prove by induction.
Base case; $n = 2$, 2 is prime, done.
Suppose it is true for all integers $1 < r \leq n$; we will prove for $n + 1$.[28]

- If $n + 1$ is prime, we are done.
- Else, $n + 1$ has a non-trivial factorization, $n + 1 = r \cdot s$, where $1 < r \leq n, 1 < s \leq n$. By induction, there exists primes p_i, q_i such that $r = p_1 \cdots p_a$ and $s = q_1 \cdots q_b$. We can then write

$$n + 1 = r \cdot s = p_1 \cdots p_a q_1 \cdots q_b,$$

a product of primes, and so we are done.

■

Definition 7.4 (Empty Product). *1; when we say $n = p_1 \cdots p_a, 0 \leq a$, a product of primes, a = 0, empty product, means $n = 1$.*

Corollary 7.1. *Any non-zero integer n is of the form*

$$\epsilon \cdot p_1 \cdots p_a, \quad \epsilon \in \{\pm 1\},$$

where p_i are primes numbers, $a \geq 0$.

Proof. If $n > 1$, this is the Lemma 7.2 where $\epsilon = 1$. If $n < -1$, the by Lemma 7.2,

$$-n = p_1 \cdots - p_n$$

so $n = -1 p_1 \cdots p_a = -p_1 \cdots p_a$. ■

Theorem 7.4 (Sieve of Eratosthenes). *Let $n > 1$ be an integer. If n is not prime, then n is divisible by some prime $1 < p \leq \sqrt{n}$.*

Sketch Proof. $n = p_1 \cdots p_a$. n not prime, $a \geq 2$. If each $p_i > \sqrt{n}$, then $p_1 p_2 \cdots p_a < \sqrt{n} \cdot \sqrt{n} = n, \perp$ ■

Lemma 7.3. *Let $p > 1$ be an integer. The following are equivalent:*

1. *p is prime*
2. *If $p | ab$, product of two nonzero integers, then $p | a$ or $p | b$.*

Proof. Assume 2., suppose $p = st \in \mathbb{Z}$. wlog, $s, t > 0$ (else replace s by $-s$, t by $-t$). $p | st$, so by 2., say $p | s$, wlog. We can write $s = p \times w$, then $p = s \cdot t = p \cdot w \cdot t$, which are all positive integers. It must be that $w = t = 1$, and thus $s = p$. Therefore, p has no non-trivial factorizations and is thus prime.
Assume now that 1. holds; $p | ab$. If $p | a$, we are done.
Suppose $p \nmid a$. Then, $\gcd(p, a) = 1$ (since only divisors of p are 1, p, so gcd could only be $1, p$, but if $\gcd = p$ then $p | a$ which is not the case). From a property of gcd's, we can write $1 = up + va$ for some $u, v \in \mathbb{Z}$. Multiplying this by b, we have $b = upb + vab$.
We have

$$\begin{aligned} p | ab &\implies p | vab \\ p | p &\implies p | upb \\ &\implies p | (upb + vab), \text{ so } p | b \end{aligned}$$

[28] Complete induction...

■

Corollary 7.2. *Let p be prime. Suppose $p|a_1a_2a_3\cdots a_m$ where $a_i \in \mathbb{Z}, m \geq 1$. Then, $p|a_i$ for some i*

Proof. By induction; we just showed the case $m = 2$. Suppose it is true for $m \geq 2$ and $p|a_1a_2\cdots a_{m+1}$; then, $p|\underbrace{(a_1a_2\cdots a_m)}_{(i)} \cdot \underbrace{a_{m+1}}_{(ii)}$. Then, either $p|(i)$ or $p|(ii)$, so $p|a_{m+1}$ or $p|a_i, 1 \leq i \leq m$, as required. ■

Theorem 7.5 (Fundamental Theorem of Arithmetic)**.** *Let $n \in \mathbb{Z}, n \neq 0$. There exists $\epsilon \in \{\pm 1\}$ and prime numbers $p_1, \cdots, p_a, a \geq 0$ such that $n = \epsilon \cdot p_1 \cdots p_a$,* ***uniquely****.*[29]

Proof. First, it is clear that the sign is unique, so wlog, we only consider positive n. We have already proved that $\exists$ such a factorization by Lemma 7.2; we now aim to show that this is unique. We proceed by induction.
Base case: $n = 1$; $p_i, q_j \geq 2$, only option is the empty product $a = b = 0$.
Assumption: say holds for integers $1 \leq m \leq n - 1, n \geq 2$ (numbers smaller than n). We are given

$$n = p_1 \cdots p_a = q_1 \ldots q_b.$$

- Suppose $p_1 = q_1$. Then $m = \frac{n}{p_1} = p_2 \cdots p_a = q_2 \cdots q_b \implies a = b$ and $p_i = q_i$ for $2 \leq i \leq a$ (and also, $p_1 = q_1$) (covered by inductive hypothesis)
- Otherwise, $p_1 \neq q_1$, and wlog (symmetric) $p_1 < q_1$. We have $p_1|n$ so $p_1|q_1 \cdots q_b \overset{p \text{ prime}}{\implies} p_1|q_i$ for some $1 \leq i \leq b$ (by Lemma 7.3, extended to the product of any number of numbers). As p_i prime, $p_1 = q_i$, implying $p_1 < q_1 \leq q_2 \leq \cdots q_i = p_1$, a contradiction to the assumption that $p_1 < q_1$. Thus, $p_1 = q_1$.

Alternatively, we could write $n = \epsilon p_1^{a_1} \cdots p_s^{a_s}$ where p_i are distinct prime numbers and $a_i > 0$ (ie, we are "collecting" the identical primes, and raising them to the power of how many times they appear) where p_i and a_i are unique. ■

Theorem 7.6 (Version of FTA for Rationals)**.** *Let $q \neq 0$ be a rational number. Then, $\exists$ a unique sign $\epsilon \in \{\pm 1\}$, integer s, primes $p_1, \ldots, p_a$ and exponents $a_i \in \mathbb{Z}, a_i \neq 0$ s.t.*

$$q = \epsilon \cdot p_1^{a_1} \cdots p_s^{a_s}$$

Proof. Write $q = \frac{m}{n}$, where $m, n \in \mathbb{Z}$. Then, we can write m as

$$m = \epsilon_m \cdot p_1^{b_1} \cdots p_s^{b_s}; \qquad n = \epsilon_n \cdot p_1^{c_1} \cdots p_s^{c_s}$$

[29] Sketch: this shows only uniqueness, existence is proven by Lemma 7.2. Use induction; base case, $n = 2$ trivial. Use complete induction, and proceed by contradiction (kind of). Assume that n has two distinct prime factorizations. Then, break down by cases; $p_1 = q_1$ or not. If they are, then take some small m covered by inductive assumption, set equal to $\frac{n}{p_1}$, meaning that if $p_1 = q_1$, the remaining $p_i = q_i$.
For inequality, show that $p_1 < q_1 \implies p_1 < p_1$ by showing that $p_1|q_1 \cdots$, and thus $p_1 = q_i$ for some i, so $p_1 < q_1 \leq \cdots q_i = p_1$, and thus you have a contradiction.

Remark 7.5. *If we allow 0 as an exponents, we can write these such that the same primes appear in both n and m.*

We can then write
$$\frac{m}{n} = \frac{\epsilon_m}{\epsilon_n} p_1^{b_1 - c_1} \cdots p_s^{b_s - c_s}.$$
We can now omit the primes with $b_i - c_i = 0$ to get only non-zero exponentiated primes. We have thus shown existence
To show uniqueness, we can disregard the sign as before. Say $0 < q = p_1^{a_1} \cdots p_s^{a_s} = p_1^{a_1'} \cdots p_s^{a_s'}$. If these are equivalent representations, then letting $c_i = a_i - a_i'$, we get that $1 = p_1^{c_1} \cdots p_s^{c_s}$; thus, we aim to show that $c_1 = \cdots c_s = 0$. wlog, we can rearrange these c's such that $c_1, \cdots, c_t < 0, c_{t+1}, \cdots, c_s \geq 0$. This implies that $p_1^{-c_1} \cdots p_t^{-c_t} = p_{t+1}^{c_{t+1}} \cdots p_s^{c_s}$. This is an equality on integers, and as given by FTA, this is only possible if $c_i = 0 \forall i$. ■

Proposition 7.1. $\sqrt{2} \notin \mathbb{Q}$

Proof. Suppose it is. Then $\sqrt{2} = p_1^{a_1} \cdots p_s^{a_s}, a_i \neq 0, p_i$ distinct primes. Then, we have
$$2 = (p_1^{a_1} \cdots p_s^{a_s})^2 = p_1^{2a_1} \cdots p_s^{2a_s}.$$
But, $2 = 2^1$, and by uniqueness of factorization, we get a contradiction because $1 \neq 2a_i$ for any i. ■

Theorem 7.7. *There exist infinitely many prime numbers.*

Proof. Suppose $p_1, \dots, p_n$ are distinct prime numbers. Then, there exists a prime number p_{n+1} which is not one of these. Let $N = p_1 p_2 \cdots p_n + 1 > 1$, so $\exists p | N$ where p prime. If $p =$ on of $p_1 \dots p_n$, say some p_i; then, $p|N$ and $p | p_1 p_2 \cdots p_n \implies p | (N - p_1 \cdots p_n) \implies p | 1$, which is a contradiction. ■

Proposition 7.2. *Let $a, b \neq 0, a, b \in \mathbb{Z}$. Then $a|b \iff a | \epsilon p_1^{a_1} \cdots p_m^{a_m}, a_1 > 0, p_i$ prime, $\epsilon \in \{\pm 1\}$ and $b = \mu p_1^{a_1'} \cdots p_m^{a_m'} q_1^{b_1} \cdots q_t^{b_t}, a_i' \geq a_i, q_i$ primes, $b_i > 0$.*

Proof. If we can, then $\frac{b}{a} = \underbrace{\frac{\mu}{\epsilon} \cdot p_1^{a_1' - a_1} \cdots p_m^{a_m' - a_m} q_1^{b_1} \cdots q_t^{b_t}}_{:=c} \implies b = a \cdot c \implies a | b$.

If $a|b$ so $b = a \cdot d$. We can write $a = \epsilon p_1^{a_1} \cdots p_m^{a_m}$, and $d = \epsilon' p_1^{r_1} \cdots p_m^{r_m} q_1^{b_1} \cdots q_t^{b_t}$, and let $b = (\epsilon\epsilon') p_1^{a_1 + r_1} \cdots p_m^{a_m + r_m} q_1^{b_1} \cdots q_t^{b_t}$ (where $r_i > 0$), and let $a_i' = a_i + r_i \geq a_i$. ■

Corollary 7.3. *Let $n = \epsilon p_1^{a_1} \cdots p_t^{a_t} \in \mathbb{Z}$, $\epsilon = \pm 1$, p_i distinct primes, $a_i > 0$. Then the divisors of n are precisely the integers*
$$\mu p_1^{c_1} \cdots p_t^{c_t}, \quad \mu = \pm 1, 0 \leq c_i \leq a_i.$$

Remark 7.6. *Let $a, b \in \mathbb{Z} \setminus \{0\}$; we write*

$$a = \epsilon p_1^{a_1} \cdots p_t^{a_t}, b = \mu p_1^{b_1} \cdots p_t^{b_t}.$$

We have $d = \gcd(a, b) = p_1^{\min(a_1,b_1)} \cdots p_t^{\min(a_t,b_t)}$.
Theorem 7.2 also follows naturally from this manner of thinking, and can be proved accordingly.

Example 7.4. $90 = 2 \cdot 3^2 \cdot 5 \cdot 7^0; 210 = 2 \cdot 3 \cdot 5 \cdot 7$. $\gcd(90, 210) = 2 \cdot 3 \cdot 5 \cdot 7^0 = 30$✓.

III. Congruences and Modular Arithmetic

8 Congruence Relations

8.1 Definitions

Definition 8.1. *Fix $n \geq 1, n \in \mathbb{Z}$. We define a relation of $\mathbb{Z}$ by $x \sim y$ if $n|(x - y)$.*

Example 8.1. *$n = 2$; $x \sim y$ if they have the same parity, ie both even or both odd.*

Lemma 8.1. *The above relation is an equivalence relation. We will denote the equivalence class of an integer r by $\overline{r}$. Then,*

$$\overline{r} = \{\ldots r - 2n, r - n, r, r + n, r + 2n, \ldots\}.$$

The set

$$\{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}$$

is a complete set of representatives.

Proof. We first show that the relation is an equivalence relation:
Reflexive: $x - x = 0 \implies n|(x - x) \forall n$, so $x \sim x$.
Symmetric: say $x \sim y \implies n|(x - y) \implies n| - (x - y) \implies n|(y - x) \implies y \sim x$.
Transitive: say $x \sim y, y \sim z \implies n|(x - y), n|(y - z) \implies n|((x - y) + (y - z)) \implies n|(x - z) \implies x \sim z$.
Now, we show that the described set is a complete set of representatives, ie we aim to show

1. *any $x \in \mathbb{Z}$ belongs to some $\overline{r}, 0 \leq r \leq n - 1$.*

   Proof of 1: Given $x \in \mathbb{Z}$, we can write $x = q \cdot n + r, 0 \leq r \leq n-1$, and $x - r = q \cdot n \implies n|(x - r)$, so $x \sim r$. Ie, $x \in \overline{r}$.

2. *if* $0 \leq r \leq s \leq n-1$ *and* $\overline{r} = \overline{s}$, *then* $r = s$ *(no repetitions, ie "repeat representation").*

   Proof of 2: If $\overline{r} = \overline{s}$, then $r \in \overline{r}$ and $r \in \overline{s}$, so $r \sim s$. So, $n | (s-r)$; but $0 \leq s-r \leq n-1 < n$, implying $s - r = 0 \implies s = r$ (since it must be a multiple of n, but less than n).

■

Example 8.2. *For* $n = 2$*, we have two equivalence classes,* $\overline{0} =$ *evens* $= \{2x : x \in \mathbb{Z}\}, \overline{1} =$ *odds* $= \{2x + 1s : x \in \mathbb{Z}\}$.

For $n = 3$*, we have three;* $\overline{0} = \{3x : x \in \mathbb{Z}\}, \overline{1} = \{1 + 3x : x \in \mathbb{Z}\}, \overline{2} = \{2 + 3x : x \in \mathbb{Z}\}$.

Definition 8.2. $x \sim y$*, we say* x *is congruent to* y *modulo* n*, and write*

$$x \equiv y \mod n.$$

Definition 8.3. *We use* $\mathbb{Z}/n\mathbb{Z}$ *or* $\mathbb{Z}_n$ *to denote the collection of congruence classes* $\mod n$*, ie* $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$.

Theorem 8.1. $\mathbb{Z}/n\mathbb{Z}$ *is a commutative ring with* n *elements. It is a field iff* n *is prime.*

We often denote $\mathbb{Z}/p\mathbb{Z}$ *where* p *prime as* $\mathbb{F}_p$.

Proof. We define $\overline{r} + \overline{s} = \overline{r+s}, \overline{r} \cdot \overline{s} = \overline{rs}$. This is well defined; meaning if we use other representatives r', s', we'll get the same result. Ie, given $r \sim r', s \sim s'$, we need to show $\overline{r' + s'} = \overline{r+s}, \overline{r' \cdot s'} = \overline{r \cdot s}$, ie $n | ((r+s) - (r'+s')), n | (rs - r's')$.
$(r+s) - (r'+s') = (r - r') + (s - s')$; both $r - r'$ and $s - s'$ are divisible by n, so we can write $rs - r's' = r(s-s') + s'(r - r')$; this whole thing is divisible by n. Now, we can verify the axioms:

1. $\overline{r} + \overline{s} = \overline{s} + \overline{r}; \overline{r} + \overline{s} = \overline{r+s} = \overline{s+r} = \overline{s} + \overline{r}$ *(commutativity of addition)*

2. . . .

3. $\overline{0}$ is the neutral element; $\overline{0} + \overline{r} = \overline{0+r} = \overline{r}$ *(neutral addition element)*

4. $\overline(r) + \overline{(-r)} = \overline{(-r)} + \overline{r} = \overline{0}$ *(inverse wrt addition)*

5. . . .

6. $\overline{1} \cdot \overline{r} = \overline{r}$

7. . . .

We now aim to show that $\mathbb{Z}/n\mathbb{Z} \iff n \in \mathbb{P}$. Suppose n composite, namely $na \cdot b$, $1 < a < n, 1 < b < n$. Note that $\overline{a}, \overline{b} \neq \overline{0}$; but, $\overline{a} \cdot \overline{b} = \overline{a \cdot b} = \overline{n} = \overline{0}$. If $\mathbb{Z} \setminus n\mathbb{Z}$ is a field, then $\exists \overline{y}$ s.t. $\overline{y} \cdot \overline{a} = \overline{1}$. We have $(\overline{y} \cdot \overline{a}) \cdot \overline{b} = \overline{1} \cdot \overline{b} = \overline{b}$, but $\overline{y} \cdot (\overline{a} \cdot \overline{b}) = \overline{y} \cdot \overline{0} = \overline{0}$, a contradiction.

Suppose, now, $n \in \mathbb{P}$. To show $\mathbb{Z}/n\mathbb{Z}$ is a field; let $\overline{a} \neq \overline{0} \in \mathbb{Z}/n\mathbb{Z}$, that is $n \not| a$. But n is prime, so $\gcd(a,n) = 1$, so $\exists u, v \in \mathbb{Z}$ such that $1 = ua + vn$. But this means

$$n|(1-ua) \implies ua \equiv 1 \mod n \implies \overline{u} \cdot \overline{a} = \overline{1} \in \mathbb{Z}/n\mathbb{Z},$$

and we have thus found a multiplicative inverse. ■

Example 8.3. *$n = 2$; we have*

+	0	1
0	0	1
1	1	0

and

×	0	1
0	0	0
1	0	1

; $\overline{1} + \overline{1} = \overline{2} = \overline{0}$.

Example 8.4. *$n = 3$; we have*

+	0	1	2
0	0	0	0
1	1	2	0
2	2	0	1

and

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

; $\overline{2} + \overline{2} = \overline{4} = \overline{1}$.

Lemma 8.2. *Let R be a commutative ring. If R has zero divisors then R is not a field.*

Proof. Let $x \neq 0$ be a zero divisor, and $y \neq 0$ s.t. $xy = 0$. If R a field, then $\exists z \in R$ s.t. $zx = 1$. But then, $z(xy) = z \cdot 0 = 0$, and $z(xy) = (zx)y = 1 \cdot y = y$, hence y must be 0, a contradiction. ■

Definition 8.4 (Unit)**.** *An element x in a ring R is called a* unit *if $\exists y \in R$ such that $xy = yx = 1$.*

Example 8.5. *If R a field, then any nonzero $x \in R$ is a unit. If $R = \mathbb{Z}/6\mathbb{Z}$, then $2, 3, 4$ are not units, but 1 and 5 are units.*

Proposition 8.1. *Take $n > 1$. An element $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ is a unit iff $\gcd(a,n) = 1$.*

Proof. Note: $\gcd(a,n) = 1$ depends only on the congruence class $\overline{a}$; $\gcd(a+kn, n) = \gcd(a,n)$. Suppose $\overline{a}$ is a unit, ie $\exists \overline{y} \in \mathbb{Z}/n\mathbb{Z}$ s.t. $\overline{y} \cdot \overline{a} = \overline{1} \implies \overline{ya} = \overline{1} \implies ya - 1 = k \cdot n$, for some $k \in \mathbb{Z}$, ie $ya - kn = 1$. Thus, if $d|a$ and $d|n$, then $d|1 \implies d = \pm 1 \implies \gcd(a,n) = 1$. Conversely, suppose $\gcd(a,n) = 1$. Then, $\exists u, v \in \mathbb{Z}$ s.t. $ua + vn = 1 \implies \overline{u} \cdot \overline{a} + \overline{vn} = \overline{1}$. Now, $\overline{n} = \overline{0} \implies \overline{v} \cdot \overline{n} = \overline{0}$, so $\overline{u} \cdot \overline{a} = 1$, hence $\overline{a}$ is a unit. ■

Corollary 8.1. *If n is prime any $\overline{a} \neq \overline{0}$ is a unit.*

8.2 Binomial Coefficients

Definition 8.5 (Binomial Coefficient)**.** *Let $m \geq n$ be non-negative integers. $\binom{m}{n}$ (m choose n) ways to choose m objects among n objects, where order doesn't matter, where $\binom{m}{n} = \frac{m!}{n!(m-n)!}$.*

We also have that

$$\binom{n}{l} + \binom{n}{l-1} = \binom{n+1}{l}$$

$$\begin{array}{ccccccc} & & & \binom{0}{0} & & & \\ & & \binom{1}{0} & & \binom{1}{1} & & \\ & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & \\ \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} \end{array}$$

Pascal's Triangle

Lemma 8.3. *Let $p \in \mathbb{P}$, and let $1 \leq n \leq p-1$. Then,*

$$p| \binom{p}{n}$$

.

Proof. First note that if $1 \leq a \leq p-1, p \not| a!$. If $p|a! = 1 \cdot 2 \cdot 3 \cdots a$, then $p|b$ where $b = \{1, 2, \dots a\}$. But we have that $1 \leq b \leq p$, so this is not possible.

Now, we have $\binom{p}{n} = \frac{p!}{n!(p-n)!} = d \in \mathbb{Z} \implies p! = d \cdot n!(p-n)!$. As $p|p!$ and $p \not| n!$ nor $(p-n)!$, (as shown above) since $n \leq p-1, p-n \leq -1$, so, since p prime, $p|d$. ■

8.3 Solving Equations in $\mathbb{Z}/n\mathbb{Z}$

Definition 8.6.

8.3.1 Linear Equations

8.4 Fermat's Little Theorem

Theorem 8.2 (Fermat's Little Theorem). *Let p be a prime number. Let $a \not\equiv 0 \mod p$ then*

$$a^{p-1} \equiv 1 \mod p.$$

Remark 8.1. *This implies that, for every a, $a^p \equiv a \mod p$. Conversely, If $a \not\equiv 0 \mod p$, then $a^p \equiv a \mod p \implies a^{p-1} \equiv 1 \mod p$ by multiplying both sides with the congruence class b s.t. $ba \equiv 1 \mod p$.*

Lemma 8.4. *Let R be a commutative ring and $x, y \in R$. Interpret $\binom{n}{i}$ as adding 1 to itself $\binom{n}{i}$ times. Then, the binomial formula holds in R, ie*

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}.$$

Ie, $\binom{n}{j}$ means $1_R + \cdots + 1_R$, $\binom{n}{j}$ times.

Proof. (Of Lemma 8.4) We proceed by induction. Case $n = 1$, clear; $(x+y)^1 = x^1 + y^1 \checkmark$.
Assume it holds for n. We write

$$(x+y)^{n+1} = (x+y)^n(x+y) = \underbrace{\left(\sum_{j=0}^{n} \binom{n}{j} x^{n-j}y^j\right)}_{\text{assumption}} \cdot (x+y)$$
$$= \sum_{l=0}^{n+1} c_l x^{n+1-l} \cdot y^l$$

where $c_l = \underbrace{\binom{n}{l}}_{\text{from } \binom{n}{l} x^{n-l}y^l x} + \underbrace{\binom{n}{l-1}}_{\text{from } \binom{n}{l-1} x^{n-(l-1)}y^{l-1}y} = \binom{n+1}{l}$, hence $(x+y)^{n+1} = \sum_{l=0}^{n+1} \binom{n+1}{l} x^{n+1-l}y^l$.

■

Proof. (Of Fermat's Little Theorem) We aim to show that $a^p \equiv a \mod p$ for any a. It is sufficient to show that it holds for $1 \le a \le p-1$.
We prove by induction on $1 \le a \le p-1$. $a = 1 \implies 1^p \equiv 1 \mod p$.

Suppose it holds for $1 \leq a \leq p-2$, and prove for $a+1$. Then, by Lemma 8.4,

$$\begin{aligned}
(a+1)^p &= \sum_{i=0}^{p} \binom{p}{i} a^i && (1)\\
&\equiv a^p + \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \cdots + \binom{p}{p-1} a + 1 && (2)\\
&\equiv 1 + a^p \quad \text{(by Lemma 8.3)} && (3)\\
&\equiv 1 + a \quad \text{by induction hypothesis} && (4)
\end{aligned}$$

Since $1+a \not\equiv 0 \mod p$, it has an inverse in $y \in \mathbb{F}_p$, $y(1+a) \equiv 1$. Then, $y(1+a)^p \equiv y(1+a) \equiv 1$. Also, $y(1+a)^p = y(1+a)(1+a)^{p-1} \equiv (1+a)^{p-1}$, hence $(1+a)^{p-1} \equiv 1$. ■

Example 8.6 (Application of Fermat's Little Theorem). *Calculate* $2^{2023} \cdot 3^9 \mod 7$. *Divide* 2023 *by* $6 = 7-1 = p-1$ *with residue.* $2023 = 6 \cdot 337 + 1$, *and* $9 = 1 \cdot 6 + 3$.

$2^{2023} \cdot 3^9 = 2(2^6)^{337} \cdot 3^6 \cdot 3^3$. *By FLT, this is equivalent to* $2(1)^{337} \cdot 1 \cdot 3^3 \equiv 2 \cdot 27 \equiv 54 \equiv 5 \mod 7$.

IV. Arithmetic of Polynomials

9 Analog to Integers

9.1 Definitions

Definition 9.1 (Polynomial Ring). *Let* $\mathbb{F}$ *be a field, and let* $\mathbb{F}[x]$ *be the ring of polynomials with coefficients in* $\mathbb{F}$, *ie*

$$\mathbb{F}[x] = \{a_n x^n + \cdots a_1 x + a_0 : a_i \in \mathbb{F}\}.$$

Operations of addition, multiplication are defined as is familiar.

Example 9.1. $\mathbb{F} = \mathbb{Z}/3\mathbb{Z}$. *We have*

$$\begin{aligned}
(x^2+x+1)(2x+1) + 2x^2 + 5 &\equiv 2x^3 + \cancelto{0}{(1+2)}x^2 + \cancelto{0}{(1+2)}x + 1 + 2x^2 + 6\\
&\equiv 2x^3 + 2x^2 + \cancel{6} \mod 3
\end{aligned}$$

Definition 9.2 (deg). *If* $f = a_n x^n + \cdots a_1 x + a_0$ *has* $a_n \neq 0$, *we say* $\deg f = n$, *unless* $f = 0$, *where* $\deg f$ *undefined.*

If f, g *not zero, then* $\deg(f \cdot g) = \deg(f) + \deg(g)$; *thus, if* f, g *are not zero,* $f \cdot g \neq 0$. *If* $f \cdot g = 0$, *we must have either that* $f = 0$ *or* $g = 0$, *or both. Thus, this is a commutative ring with no zero divisors.*

Theorem 9.1 (Division with Residue)**.** *Let $f, g \in \mathbb{F}[x]$, $g \neq 0$. Then, $\exists!$ polynomials $g, r \in \mathbb{F}[x]$ s.t. $f = q \cdot g + r$, where either $r = 0$ or $\deg(r) < \deg(g)$; furthermore, q, r are unique.*

Proof. If $f = 0$, then take $q = 0, r = 0$ (no other choice). Take $f \neq 0$ wlog. We first prove *existence* by induction on $\deg f$.

- *Base:* $\deg f = 0$: If $\deg g > 0$, let $q = 0$, $r = f$, hence $f = 0 \cdot g + f$. Otherwise, if $\deg g = 0$, then g is a constant, then $f = (fg^{-1}) \cdot g + 0$.
- *Assumption:* suppose true for all polynomials $h \in \mathbb{F}[x]$ such that $\deg h \leq n$ and $\deg f = n + 1$. Say $f = a_{n+1}x^{n+1}+$ l.o.t.[30], and $g = b_m x^m+$ l.o.t., where $b_m \neq 0$.
  - If $n + 1 < m$, then $f = 0 \cdot g + f$, $\deg f < \deg g$.
  - If $n + 1 \geq m$, then $f(x) = \underbrace{a_{n+1}b_m^{-1}x^{n+1-m}g}_{=a_{n+1}x^{n+1}+\text{ l.o.t}} + h(x)$, where h is essentially the "difference" between the expression. Note that $\deg h \leq n$; hence, by induction $h(x) = \tilde{q}(x) \cdot g(x) + r(x)$, where either $r(x) = 0$ or $\deg r < \deg g$. This implies that

$$f(x) = \underbrace{\left(a_{n+1}b_m^{-1}x^{n+1-m} + \tilde{q}(x)\right)}_{q(x)} g(x) + r(x).$$

Thus, the proof holds for all $\deg f$. We know show uniqueness. Suppose $f = q_1 g + r_1 = q_2 g + r_2$, where $r_i = 0$ or $\deg r_i < \deg g$. Consider

$$(q_1 - q_2)g = r_2 - r_1.$$

If RHS $\neq 0$, then the LHS $\neq 0$, hence $q_1 - q_2 \neq 0$. Since $g \neq 0$, then $\deg(\text{LHS}) = \deg(q_1 - q_2) + \deg g \geq \deg g$. But $\deg \text{RHS} \leq \max(\deg r_1, \deg r_2) < \deg g$, and we have a contradiction. Hence, RHS = 0 $\implies$ LHS = 0, hence $q_1 - q_2 = 0$, so $r_1 = r_2$, $q_1 = q_2$, and the polynomial is thus unique. ■

Definition 9.3 (Divisibility)**.** *We say $g|f$ if $r = 0$; namely,*

$$f = q \cdot g \text{ for some } q \in \mathbb{F}[x].$$

As before, $g|f \implies g|hf$ for any $h \in \mathbb{F}[x]$; $g|f_1, g|f_2 \implies g|(f_1 \pm f_2)$; etc. Many of the other consequences of divisibility in integers follow similarly.

9.2 GCD

Definition 9.4 (GCD of Polynomials)**.** *Let $f, g \in \mathbb{F}[x]$ not both 0. The greatest common divisor of f, g denoted $\gcd(f, g)$ is a* monic *polynomial of largest degree dividing both f and g.*

[30] Lower order terms

Definition 9.5 (Monic). *$f = a_n x^n + \cdots + a_0$, $a_n \neq 0$ is monic if $a_n = 1$ (leading term is one).*

Theorem 9.2 (GCD). *$\gcd(f, g)$ exists and is unique. Furthermore, of the nonzero monic polynomials of the form*

$$u(x)f(x) + v(x)g(x),$$

it has the minimal degree. Any common example of f, g divides the gcd.

Proof.

- *Existence:* Let $S := \{a(x) : a(x) \text{ monic, nonzero}; a(x) = u(x)f(x) + v(x)g(x).\}$. $S \neq \varnothing$; if $f \neq 0$, rather $f = a_n x^n +$ l.o.t., then $a(x) = a_n^{-2} f(x) \cdot f(x) + 0 \cdot g(x) \in S$ (if $f = 0$, use g by same argument). Choose some $h(x) \in S$ have the minimal positive degree.

- *Unique:* suppose $h_1(x) \in S$ and $\deg h = \deg h_1 = d$, $h = x^d +$ lot $= uf + vg$, $h_1 = x^d +$ log $= u_1 f + v_1 g$. Now either:

  - $h - h_1 = 0$ (done)
  - $\deg(h - h_1) < \deg h$. However, $h - h_1 = (u - u_1)f + (v - v_1)g$. $h - h_1 = a_e x^e +$lot, then $ae^{-1}(h - h_1)$ is monic of $\deg < \deg h$, and is in S, a contradiction.

    Hence, h must be unique.

- $h|f, h|g$: Write

  $$f = q \cdot h + r.$$

  If $r = 0$, $h|f$. Else, $r = f - q \cdot h$, and thus $r \in S$, and we can write $r = f - q(uf + vg) = (f - qu)f - (qv)g$. Thus, after normalization (ie "divide out" to make monic), $r \in S$, and has a smaller degree then h, and we thus have a contradiction, and so $r = 0$. Thus, $h|f, h|g$.

- *Maximality of* $\deg(h)$*:* Suppose $t(x)|f, t(x)|g$, thus $t(x)|(uf + vg)$, so $t|h$. Thus, $\deg t \leq \deg h$, and further h has the maximal possible degree, hence h is the monic common divisor of max degree.

- *Uniqueness of GCD:* Say h_1 another common divisor of f, g of the same degree of h. We have that $\deg h = \deg h_1$ and $h_1|h$, and further h, h_1 monic, then $h = h_1$.

■