MATH340 Review Notes

By Jack 'jryzkns' Zhou

1 Axiomatic Approach to $\mathbb{N}$

Definition: $\mathbb{N}$ is a set with 3 axioms (sometimes referred to as the "Peano Axioms"):

1. $1 \in \mathbb{N}$
2. For every $a \in \mathbb{N}$, there is an element called the *successor* of a, written as $succ(a) = a + 1 \in \mathbb{N}$
3. Every element $a \in \mathbb{N}$ arises in this manner:

$$\mathbb{N} = \{succ^k(1) \mid k \geq 0\}$$

2 Mathematical Induction

Principle of Mathematical Induction:
Suppose $X \subseteq \mathbb{N}$ and:

1. $1 \in X$
2. $a \in X \Rightarrow a + 1 \in X$

Then $X = \mathbb{N}$.
This is taken as an axiom and cannot be proven from the 3 axioms presented in section 1.
Strong Induction:
Suppose $X \subseteq \mathbb{N}$ satusfies the properties

1. $1 \in X$
2. $\forall i \in [1, n] \;\; i \in X \Rightarrow n + 1 \in X$

This variant of induction is logically equivalent to the simple form of induction, but in a proof it may be desirable to refer to more than 1 case that is taken to be true, in which case a strong induction is preferred.
The Well-Ordering Principle (WP):
Every non-empty subset $Y \subseteq \mathbb{N}$ has a minimal element.
We can use WP to prove the Principle of Induction:
Suppose $X \subseteq \mathbb{N}$ has the properties $1 \in X$ and $k \in X \Rightarrow k + 1 \in X$, WTS $X \in \mathbb{N}$. Suppose $Y = \{n \in \mathbb{N} \mid n \notin X\}$, then $X = \mathbb{N} \Leftrightarrow Y = \varnothing$
We proceed to show that $Y = \varnothing$ by contradiction, assuming $Y \neq \varnothing$. By WP, Y has a minimum element $n^* \in Y$. As $1 \notin Y$ (because $1 \in X$), $n^* > 1$ so $n^* - 1 \in \mathbb{N}$ and $n^* - 1 \notin Y$ because n^* is the minimal element of Y. Therfore $n^* - 1 \in X$, but then $succ(n^* - 1) = n^* - 1 + 1 = n^* \in X$ by the inductive hypothesis. As $n^* \in Y$, we have come to a contradiction, and therefore $Y = \varnothing$ and $X = \mathbb{N}$.
Note: WP is false for other sets of numbers. For example, there is no minimal element in $\mathbb{R}^+$ as $\forall x \in \mathbb{R}^+ \;\; \frac{1}{2}x < x$.

3 Operations on $\mathbb{N}, \mathbb{Z}$

Multiplication on $\mathbb{N}$:
Inductively defined with $1 \cdot a := a$ as the base case. If $n \cdot a$ is defined, then $(n + 1) \cdot a := n \cdot a + a$.
The Peano Axioms imply the following properties:

- Commutativity: $ab = ba$
- Associativity: $a(bc) = (ab)c$
- Distribution over Addition: $a(b + c) = ab + ac$

Defining $\mathbb{Z}$ from $\mathbb{N}$
Suppose we want to solve an equation like $x + 5 = 2$ in $\mathbb{N}$, there are no solutions, because $x = 2 - 5 \notin \mathbb{N}$. Therefore, we need to invent the notion of negative numbers.
To do this, we can say that $\mathbb{Z}$ is the set $\mathbb{N} \times \mathbb{N} = \{(a, b) \mid a, b \in \mathbb{N}\}$ with an equivalence relation $(a, b) = (a + c, b + c)$ for any $a, b, c \in \mathbb{N}$. The ordered tuple (a, b) represents $a - b$. We can see that $(a + c) - (b + c) = a - b$. More concretely, consider $(5, 0) = (6, 1) = (500, 495)$ and $5 - 0 = 6 - 1 = 500 - 495$. A negative number $-a$ could then be represented as $(0, a)$.
Induction in $\mathbb{Z}$
WP does not apply to $\mathbb{Z}$, so in practice we either treat +ive and -ive numbers separately, or we go by the absolute value of the numbers.

4 The Division Theorem in $\mathbb{Z}$

Theorem:
Let $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. Then there exists unique $q \in \mathbb{Z}, r \in (0, b)$ such that $a = qb + r$.
Proof: We proceed in two steps, showing existence then uniqueness.
Existence: We have $a \in \mathbb{Z}, b \in \mathbb{N}$, we define

$$X = \{n \in \mathbb{N} \cup \{0\} \mid n = a - qb\}$$

For some integer q. X is nonempty as $a - qb \geq 0$ by choice of q. If $a > 0$, we pick $q = 0$. If $a \leq 0$, we pick $q = a$. By WP, X has a minimal element that we will call r; $r = a - qb$ for some $q \in \mathbb{Z}$. Since $r \in \mathbb{N} \cup \{0\}$, $r \geq 0$. r also satisfies $r < b$. If $r \geq b$, then $r - b \in X$ as $r - b = (a - qb) - b = a - (q + 1)b$. This contradicts minimality of r. Rearranging $r = a - qb$ we get $a = qb + r$.
Uniqueness: Suppose we have (q_1, r_1) and (q_2, r_2) both satisfying the theorem, WTS $q_1 = q_2$ and $r_1 = r_2$.
We have $a = q_1 b + r_1 = q_2 b + r_2$ with $r_1, r_2 \in (0, b)$. If we collect the terms with b on one side, we have $(q_1 - q_2)b = r_2 - r_1$. So, $r_2 - r_1$ is a multiple of b. Given the constraint $r_1, r_2 \in (0, b)$, we can see that $r_2 - r_1 \in [-(b - 1), (b - 1)]$. Therefore it is only possible that $r_2 - r_1 = 0$ is a multiple a multiple of b. Therefore $r_2 = r_1$ and $(q_1 - q_2)b = 0 \Rightarrow q_1 = q_2$.

4.1 What if $b < 0$?

$a = qb + r \Leftrightarrow a = (-q)(-b) + r$. The theorem still works, but $0 \geq r \geq |b|$ needs to be guaranteed.

5 Divisibility in $\mathbb{Z}$

Definition: Let $d, a \in \mathbb{Z}$, we say that d divides a, written as $d|a$, if $a = qd$ for some $q \in \mathbb{Z}$.
Equivalently: d is a *divisor* of a, a is a *multiple* of d, or a is *divisible* by d.
Some Facts:

- $\forall d \in \mathbb{Z}\ \ d|0$ but $0 \nmid a$ unless $a = 0$.
- If d divides $a \neq 0$ then $|d| \leq |a|$. In particular, the set of divisors of a non-zero integer is finite.
- $d|a \Leftrightarrow |d| \mid |a|$

6 GCD in $\mathbb{Z}$

Definition: Let $a, b \in \mathbb{Z}$, not both 0. The *greatest common divisor* of a and b, $\gcd(a, b)$ is the greatest $d \in \mathbb{Z}$ such that $d|a$ and $d|b$.
Lemmas:

- $(d|a \wedge d|b) \to d|(a-b)$
- $(d|(a-b) \wedge d|b) \to d|a$

Note that these lemmas mean that if d is a common divisor of (a, b) then it is equivalent to d is a common divisor of $(b, a-b)$; $\gcd(a, b) = gcd(b, a-b)$.

7 Bezout's Identity in $\mathbb{Z}$

Theorem:
Let $g = \gcd(a, b)$. Then $g = ax + by$ for some $x, y \in \mathbb{Z}$.
Proof: Suppose we have two sets:

$$\begin{aligned} D &= \{d \in \mathbb{Z} \mid d|a \wedge d|b\} \\ I &= \{ax + by \mid x, y \in \mathbb{Z}\} \end{aligned}$$

D is the set of all common divisors between a, b and I is the set of all integer combinations of a, b.
From this we make claim (1): If $d \in D$ and $n \in I$, then $d|n$. In particular, if $n \neq 0$, $|d| \leq |n|$.
Since $d \in D$, we have $a = q_1 d$ and $b = q_2 d$ for some $q_1, q_2 \in \mathbb{Z}$. Similarly, since $n \in I$, we have $n = ax + by$ for some $x, y \in \mathbb{Z}$. We can see that $n = ax + by = q_1 dx + q_2 dy = d(q_1 x + q_2 y) \Rightarrow d|n$.
Suppose now we look at $I \cap \mathbb{N}$, the integer multiples of a, b that are natural numbers, we let $n^* = \min(I \cap \mathbb{N}) = ax^* + by^*$.
We proceed to make claim (2) that $n^*|a$ and $n^*|a$ (i.e. $n^* \in D$).
Suppose $n^* \nmid a$, we divide a by n^* to get $a = qn^* + r$, $r \in (0, n^*)$. By definition of n^*, we see that

$$\begin{aligned} r &= a - qn^* \\ &= a - q(ax^* + by^*) \\ &= a - qax^* + qby^* \\ &= a(1 - qx^*) + b(qy^*) \end{aligned}$$

This means that $n^* \in I$ and that contradicts the minimality of n^* as $r \in (0, n^*)$.
Finally, we make our last claim (3): $n^* = \max(D) = \gcd(a, b)$. By claim (2), n^* is a common divisor of a, b. If $d \in D$ is any other common divisor, then $d \leq n^*$ by claim (1). We can see that $d \leq |d| \leq |n^*| = n^*$.
Therefore, we have two interpretations of $\gcd(a, b)$:

- $\gcd(a, b) = \max(D)$

  maximal element in set of common divisors
- $\gcd(a, b) = \min(I \cap \mathbb{N})$

  smallest positive integer combination of a, b.

8 Euclidean Algorithm

Theorem:
If $a = qb + r$, then $\gcd(a, b) = \gcd(b, r)$.
Proof:
It is given that $\gcd(a, b) = \gcd(a - b, b)$. As $r = a - qb$, we can consider applying the $a - b$ operation q times: $\gcd(a, b) = \gcd(b, a - qb) = \gcd(b, r)$.
Algorithm
Given: (a, b) with $a > b > 0$ and repeatedly apply division theorem on (a, b). After each division, we replace a with b and b with the remainder of the division:

$$\begin{aligned} (a, b) &\quad a = q_1 b + r_1 \\ (b, r_1) &\quad b = q_2 r_1 + r_2 \\ (r_1, r_2) &\quad r_1 = q_3 r_2 + r_3 \\ \vdots &\quad \vdots \\ (r_{k-2}, r_{k-1}) &\quad r_{k-2} = q_k r_{k-1} + r_k \\ (r_{k-1}, r_k) &\quad r_{k-1} = q_{k+1} r_k + 0 \\ (r_k, 0) & \end{aligned}$$

The algorithm stops when we reach a point where the second value in the tuple is 0, in which case $\gcd(a, b) = r_k$. This algorithm is guaranteed to terminate as each of the r_i up to terminating r_k are strictly decreasing natural numbers. By WP there is a minimal element to which this procedure will terminate on.

9 Factoring of Integers

Definition:
An integer $p \neq \pm 1$ is said to be *irreducible* if its only divisors are itself and 1 or -1.
Definition:
An integer $p \neq 0, \pm 1$ is said to be *prime* if for some $a, b \in \mathbb{Z}$, $p|ab$ implies $p|a$ or $p|b$.
Theorem:
If $n \in \mathbb{Z} \setminus \{0, 1, -1\}$, n is a product of irreducible integers.
Proof:
We will proceed by strong induction. The base case $n = 2$ is irreducible. In the general case, suppose $n > 2$ and the

theorem is true for all $i \in [2, n]$. If n is irreducible, then we are done. Otherwise, $n = ab$ for some $a, b \in [2, n]$, in which case $2 \geq a, b < n$ and a, b are products of primes. A product of products of primes is still a product of primes.

10 Euclid's Lemma

Lemma:
An integer p is prime if and only if p is irreducible.
Proof:
($\Rightarrow$): Let p be prime. To show that p is irreducible, suppose $p = ab$ for some $a, b \in \mathbb{Z}$, WTS a or b is ± 1. As $p = ab$, we know that $p|a$ or $p|b$. WLOG, suppose $p|a$. This means that $a = pd$ for some $d \in \mathbb{Z}$. So, $p = ab = (pd)b$. Suppose we divide $p = (pd)b$ by p, we get $1 = db$. Thereore, $d, b = \pm 1$; p is irreducible.
($\Leftarrow$): Let p be irreducible. To show that p is prime, suppose $p|ab$ for some $a, b \in \mathbb{Z}$ and show $p|a$ or $p|b$. As p is irreducible, $\gcd(p, a)$ is either 1 or p. If $\gcd(p, a) = p$, then $p|a$ and we are done. Otherwise, if $\gcd(p, a) = 1$, then by Bezout's Indentity, we have $1 = px + ay$ for some $x, y \in \mathbb{Z}$. Therefore,

$$b = b(px + ay) = pbx + aby$$

Note that $p|ab$ is equivalent to saying $ab = pn$ for some $n \in \mathbb{Z}$, we can substitute this in:

$$b = pbx + pny = p(bx + ny)$$

From this we can see that $p|b = p(bx + ny)$; p is prime.

11 Fundamental Theorem of Arithmetic

Theorem:
Let $n \in \mathbb{Z} \setminus \{0, 1, -1\}$, n is a product of prime numbers. Moreover, given two prime factorizations $n = p_1 \cdots p_k = q_1 \cdots q_l$, $k = l$ and it's possible to re-enumerate $q_1, \ldots, q_l$ so that $\forall i \;\; p_i = \pm q_i$.
Proof:
We proceed by showing existence then uniqueness.
Existence: This is already proven with a previous theorem showing that if $n \in \mathbb{Z} \setminus \{0, 1, -1\}$, n is a product of irreducible integers.By Euclid's Lemma, we can also say that such n is a product of prime integers.
Uniqueness: Suppose $n = p_1 \cdots p_k = q_1 \cdots q_l$. We proceed by induction on k. For the base case $k = 1$, we have $n = p_1 = q_1$. In the general case, suppose $n = p_1 \cdots p_{k+1} = q_1 \cdots q_l$. We look at p_1, since $p_1 | n = q_1 \cdots q_l$, then $p_1 | q_i$ for some i. Therefore $p_1 = \pm q_i$. Suppose we let let q_i swap indices with q_1, then we have $n = p_1 \cdots p_{k+1} = q_1 q_2 \cdots q_l = p_1 q_2 \cdots q_l$. We can divide $p_1 \cdots p_{k+1} = p_1 q_2 \cdots q_l$ by p_1, which leaves us with $p_2 \cdots p_{k+1} = q_2 \cdots q_l$ and we can repeat this procedure to set $p_j = \pm q_i$ for all remaining j factors in $p_2 \cdots p_{k+1}$.

12 Modular Arithmetic

Let $a\mathbb{Z}$ and $m \in \mathbb{Z} \setminus \{0\}$, where m is commonly referred to as the *modulus*, we explore some definitions:
Definition:
The *residue* of a modulo m is the remainder of a when divided by m.
Definition:
The *congruence class* of a modulo m is defined as the set

$$[a]_m := \{a' \in \mathbb{Z} \mid a \equiv a' (\text{mod } m)\}$$

We say that a is a *representative* of $[a]_m$.
Congruence classes under the same modulus m are either equal or disjoint. If $x, x' \in [a]_m$, then $x' - x | m$.
Alternatively, we can generate $[a]_m$ in the following way:

$$[a]_m = \{a + km \mid k \in \mathbb{Z}\}$$

Definition:
The integers modulo m, $\mathbb{Z}/m\mathbb{Z}$, is the set of congruence classes modulo m.

13 Algebra and Operations on $\mathbb{Z}/m\mathbb{Z}$

Definition:
In $\mathbb{Z}/m\mathbb{Z}$, addition is defined as

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

and multiplication is defined as

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

Definition:
An element x is said to be *invertible* if there exists an element y such that $[xy]_m = [1]_m$. We say x and y are multiplicative inverses
Definition:
An element x is said to be a *zero divisor* if $x \neq 0$ and there exists an element $y \neq 0$ such that $[xy]_m = [0]_m$

14 Theorems about $\mathbb{Z}/m\mathbb{Z}$

Theorem:
An element of $\mathbb{Z}/m\mathbb{Z}$ cannot be both an invertible element and a zero divisor.
Proof:
Suppose $[a]_m$ is invertible, then there exists $[a'] \in \mathbb{Z}/m\mathbb{Z}$ such that $[a]_m[a']_m = [1]_m$. Suppose that also $[a]_m[b]_m = [0]_m$ for some $b \in \mathbb{Z}/m\mathbb{Z}$. Suppose we multiply $[a]_m[b]_m = [0]_m$ by $[a']_m$, we have

$$\begin{aligned} [a]_m[b]_m &= [0]_m \\ ([a']_m[a]_m)[b]_m &= [a']_m[0]_m \\ [b]_m &= [0]_m \end{aligned}$$

Therefore, the only possible b that satisfies $[a]_m[b]_m = [0]_m$ is 0, therefore $[a]_m$ cannot be both invertible and a zero divisor.
Theorem:

In $\mathbb{Z}/m\mathbb{Z}$, multiplicative inverses are unique whenever they exist.
Proof:
Let $[a]_m \in \mathbb{Z}/m\mathbb{Z}$ be an invertible element and suppose $[a]_2$ has two inverses b_1, b_2:

$$[a]_m[b_1]_m = [1]_m \quad [a]_m[b_2]_m = [1]_m$$

We can attempt to evaluate $[b_1]_m[a]_m[b_2]_m$:

$$([b_1]_m[a]_m)[b_2]_m = [b_2]_m \quad [b_1]_m([a]_m[b_2]_m) = [b_1]_m$$

We can see that depending on the order of operations taken, we get either b_1 or b_2. but as $[b_1]_m[a]_m[b_2]_m$ is always the same value, we can conclude that $b_1 = b_2$.
Theorem:
$[a]_m$ is an invertible class $\Leftrightarrow \gcd(a, m) = 1$
Proof:
($\Rightarrow$): If $[a]_m$ is invertible, then there exists $[b]_m \in \mathbb{Z}/m\mathbb{Z}$ such that $[a]_m[b]_m = [1]_m$. We can see that $ab = 1 + km$ for some $k \in \mathbb{Z}$. We can rearrange this to $ab + (-k)m = 1$. As the $\gcd(a, m)$ is the smallest natural number to $ax + my$, we have $ab + (-k)m = 1$ so $\gcd(a, m) = 1$.
($\Leftarrow$): The same logic applies but in the reverse direction.
Theorem:
$[a]_m$ is a zero divisor $\Leftrightarrow \gcd(a, m) > 1$
Proof:
($\Rightarrow$): If $[a]_m$ is a zero divisor, $[a]_m$ is not invertible (by previous theorem: an element cannot be both invertible and zero divisor). So $\gcd(a, m) \neq 1$. As $\gcd(a, m) \in \mathbb{N}$ and $\gcd(a, m) \neq 1$, $\gcd(a, m) > 1$.
($\Leftarrow$): Suppose $\gcd(a, m) = g > 1$, let $b = m/g$. If we take the product $ab = a \cdot (m/g) = m \cdot (a/\gcd(a, m))$, we can see that $ab|m$ or $[a]_m[b]_m = [0]_m$; $[a]_m$ is a zero divisor.
Theorem:
If $[a] \in \mathbb{Z}/m\mathbb{Z}$ is invertible and $[b] \in \mathbb{Z}/m\mathbb{Z}$ is arbitrary, then the equation

$$[a]_m x = [b]_m$$

has exactly one solution. Namely, $x = [a]^{-}1_m[b]_m$.
Proof:
We can show the uniqueness of the solution by solving:

$$\begin{aligned}[a]_m x &= [b]_m \\ ([a]_m^{-1}[a]_m)x &= [a]_m^{-1}[b]_m \\ [1]_m x &= [a]_m^{-1}[b]_m\end{aligned}$$

Therefore, x must be $[a]_m^{-1}[b]_m$.

15 Invertible elements in $\mathbb{Z}/m\mathbb{Z}$

Definition:
The set of invertible elements of $\mathbb{Z}/m\mathbb{Z}$ is denoted as $(\mathbb{Z}/m\mathbb{Z})^\times$ or $(\mathbb{Z}/m\mathbb{Z})^*$:

$$(\mathbb{Z}/m\mathbb{Z})^\times = \{[a]_m \in \mathbb{Z}/m\mathbb{Z} \mid \gcd(a, m) = 1\}$$

Definition:
The cardinality of $(\mathbb{Z}/m\mathbb{Z})^\times$ is denoted $\phi(m)$, where ϕ is the Euler Totient function. ϕ has the following properties:

(1) If $\gcd(a, b) = 1$, then $\phi(a, b) = \phi(a)\phi(b)$

(2) If p is prime and $k \geq 1$, then $\phi(p^k) = (p-1)p^{k-1}$

We proceed to prove these properties of ϕ:
Proof(taken from HW3 Q2):
(1): In $\mathbb{Z}/mn\mathbb{Z}$ where $\gcd(m, n) = 1$, the element $[a]_{mn}$ is invertible if and only if $[a]_m$ and $[a]_n$ are invertible as well. Therefore, each invertible element in $(\mathbb{Z}/mn\mathbb{Z})^\times$ correspond to a pair of elements in $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$; there is a bijection betwen $(\mathbb{Z}/m\mathbb{Z})^\times$ and $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$. Therefore $\phi(mn) = \#((\mathbb{Z}/mn\mathbb{Z})^\times) = \#((\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times) = \#((\mathbb{Z}/m\mathbb{Z})^\times) \cdot \#((\mathbb{Z}/n\mathbb{Z})^\times) = \phi(m)\phi(n)$.
(2): We wish to count all elements in $\mathbb{Z}/p^k\mathbb{Z}$ that are invertible. Since we are working with a prime number p, it would be easier to count all zero-divisors instead. Namely, only the values $p, 2p, 3p, ...$ divide into p^k since p is prime. Out of a total of p^k classes, every p^{th} class is a zero divisor. Therefore there are $p^k/p = p^{k-1}$ zero divisors. Taking this amount (p^{k-1}) out of the total (p^k), we have $\phi(p^k) = p^k - p^{k-1} = (p-1)p^{k-1}$
Theorem:
If $[a]_m \in \mathbb{Z}/m\mathbb{Z}$ is invertible, then $[a]_m^{\phi(m)} = [1]_m$. Note that this implies that $[a]_m^{\phi(m)-1} = [a]_m^{-1}$ because $[a]_m^{\phi(m)-1}[a]_m = [a]_m^{\phi(m)} = [1]_m$. In the case where m is a prime number p, we have *Fermat's Little Theorem*:
If p is prime and $p \nmid a$, then $[a]_p^{p-1} = [1]_p$ in $\mathbb{Z}/p\mathbb{Z}$.
Proof:
Given $(\mathbb{Z}/m\mathbb{Z})^\times$, we multiply each element by $[a]_m$. If we get $[a]_m[a_i]_m = [a]_m[a_j]_m$, then we multiply by $[a]_m^{-1}$, ensuring every element in $[a]_m \cdot (\mathbb{Z}/m\mathbb{Z})^\times$ is distinct. If two elements are invertible, their product is invertible as well. Therefore, $[a]_m \cdot (\mathbb{Z}/m\mathbb{Z})^\times$ is just $(\mathbb{Z}/m\mathbb{Z})^\times$ with rearranged elements. Now we take the product over $[a]_m \cdot (\mathbb{Z}/m\mathbb{Z})^\times$:

$$\begin{aligned}\prod_{i \in [a]_m \cdot (\mathbb{Z}/m\mathbb{Z})^\times} i &= [a]_m^{\#((\mathbb{Z}/m\mathbb{Z})^\times)} \prod_{i \in (\mathbb{Z}/m\mathbb{Z})^\times} i \\ &= [a]_m^{\phi(m)} \prod_{i \in (\mathbb{Z}/m\mathbb{Z})^\times} i \\ &= [a]_m^{\phi(m)}[1]_m \\ &= [a]_m^{\phi(m)} \\ &= [1]_m\end{aligned}$$

Notice that as $(\mathbb{Z}/m\mathbb{Z})^\times$ contains both invertible elements are their inverses, the product over every element in $(\mathbb{Z}/m\mathbb{Z})^\times$ would simply equal to $[1]_m$. From this we can see that $[a]_m^{\phi(m)} = [1]_m$.