Chapter 1

Integers

Even though the professor started with sets, the textbook starts with integers, and I'm reading the textbook along side the class, so I'm starting here too. Integers are everywhere, we all get them intuitively after years of grade school, so it's a good choice for learning groups. This chapter is building up to what how we can use modulo to study finite groups, and I think we're gonna be using them a lot. Let's dive in.

1.1 Division

Before we can understand what it means to take a modulo, we gotta figure out how we build integers. Thats gonna involve prime numbers, but to understand why those are special we need to know what it means to divide an integer. Never mind that we need the definition of multiplication to figure that out first.

1.1.1 Definition An integer a is called a *multiple* of an integer b if $a = bq$ for some integer q. Then we say b is a *divisor* of a, and say $b|a$.

- Note: Sometimes b is called a *factor* a.
- Ex: $2|6$ is true, and equals 3.
- If $a \neq \emptyset$ and $b|a$, then $|b| \leq |a|$, since $|b| \leq |b| \cdot |q| = |a|$. From that we can see that if $b|a$ and $a|b$, $|a| = |b|$. The absolute values are used here because b, q, or a could be negative.

- $1|b$ is always true. If $b|1$ is also true, then $b = \pm 1$.
- The only multiple of 0 is 0 itself. So for $a|b$, $a = 0$ implies $b = 0$, $0|0$ However, any integer $a|0$, since $0 = a \cdot 0$.

1.1.2 Axiom The Well Ordering Principle.

This one is a big one for me, since I'm getting a little stir crazy about the deeply related, demonstrably equivalent Axiom of Choice, but since I learned about it first in class, I'm leaving the discussion of it to chapter 2.

1.1.3 Theorem (Division Algorithm). For any integers a and b, with $b > 0$, there exists unique integers q (the **quotient**) and r (the **remainder**) such that

$$a = bq + r, \ \textit{with} \ 0 \leq r < b.$$

Proof Thoughts: This proof uses the Well Ordering Principle to show that there is an r which satisfies the equation $r = a - bq, \ \textit{with} \ 0 \leq r < b$. It then uses the definition of division and some arithmetic manipulation to show that they are unique. Not gonna lie this one was a bit brain bendier for me than the other ones. I need to practice my number theory.

Proof: Lets take the set of all remainders $R = \{a - bq : a, b, q \in \mathbb{Z}, b > 0\}$. We would like to consider only the nonnegative elements, R^+. To do so we must first show that R^+ is not empty. Consider the element $j = a - bq : a, b, q \in \mathbb{Z}, b > 0, q = -|a|$. Clearly $j \in R$. Then $j = a - (-|a| \cdot b) = a + (|a| \cdot b)$, which is either b if $a \leq 0$ or $b|a \cdot -1|$ when $a \geq 0$, and since by definition $b > 0$, then so is j and $j \in R^+$. Therefore $R^+ \neq \emptyset$.

By the Well Ordering Principle, there exists some smallest element which we will call $r \in R^+$. By definition, $r \geq 0$, and $r = a - bq$ for some $a, b, q \in \mathbb{Z}$. We need to show that additionally $r < b$ to show the existence of an element that satisfies the requirements of the theorem.

We claim that we cannot have $r \geq b$, ands lets do a small proof by contradiction to show so. Let $s = r - b, s \in R^+$. It is clear that $s < r$, and since $s \in R^+, s \geq 0$. This is the contradiction. Since $s = r - b, s = a - bq - b = a - b(q + 1)$.

Finally, rearranging the construction of r to define a, we see that there must exist an $a = bq + r, 0 \leq r < b$.

To show that they are unique, suppose we had two ways of writing a in terms of b: $a = bq + r$ and $a = bp + s$. Note that $0 \leq r < b$ and $0 \leq s < b$. Then we have that $bq + r = bp + s$, $(s - r) = bq - bp = b(q - p)$. Then we can see that $b|(s - r)$, but both $r < bands < b$, and the only way for that to make sense is if $s - r = 0$. This implies that $bq - bp = 0$ so $bq = bp, q = p, s = r$, and therefore q and r are unique. We have existence and uniqueness of q and r, therefore the theorem is proven. On to the next.

1.1.4 Theorem Let $\mathcal{I}$ be a nonempty set of integers, closed under addition and subtraction. Then it contains either 0 alone, or some smallest positive element, in which case $\mathcal{I}$ contains every multiple of this element.

Proof Thoughts: So, we can work with the assumption that we're closed under addition and subtraction, $a + b \in \mathcal{I}, a - b \in \mathcal{I}$. Then we can use the Well Ordering Principle to show that it's got a smallest positive element b. Now we need to show that every multiple of that element $= \mathcal{I}$. Showing that $b\mathbb{Z} \subseteq \mathcal{I}$ is easy. The converse is the interesting part of the proof. This one is still simpler than the last one (thank god for that, for me).

Proof: Since $\mathcal{I} \neq \emptyset$, it is either $\{0\}$, or contains a non zero element, by the assumptions in the proof. In the case that $0 = \mathcal{I}$, we are done. In the second case, there is an element $a \in \mathcal{I}$, but since the set is closed by subtraction, we can see that $0 - a = -a$, so $-a \in \mathcal{I}$. Either a *or* $-a$ is positive, which means that the set $mathcalI^+$ is non-empty. By the Well Ordering Principle, we know it has a smallest element, b. Let $b\mathbb{Z}$ be the set of all multiples of b. It is clear that since $\mathcal{I}$ is closed under addition, that $b\mathbb{Z} \subseteq \mathcal{I}$.

To show that $\mathcal{I} \subseteq b\mathbb{Z}$, we must show that $\forall c \in \mathcal{I},\ b|c$. By the Division Algorithm, $c = bq + r, r = c - bq$. It is clear that $bq \in \mathcal{I}$. What about r? Well, $0 \leq r < b$, but since in our case we found b using the Well Ordering Principle, it was the smallest element in our set I^+. Therefore either $r = 0$ or $r > 0$, but if $r > 0$ it would be b, which it isn't either. So $r = 0$ and $c = bq$ so $b|c$ and therefore $c \in b\mathbb{Z}$. Therefore $\mathcal{I} \subseteq b\mathbb{Z}$, and $\mathcal{I} = b\mathbb{Z}$

1.1.5 Definition (Greatest Common Divisor) Let a and b be integers, not both zero. A positive integer d is called the {greatest common divisor} of a and b if

1. d is a divisor of both a and b. $d|a$ and $d|b$.
2. A divisor of both a and b is also a divisor of d. If $c|a$ and $c|b$, then $c|d$.

The greatest common divisor of a and b, denoted by $\gcd(a, b)$ and (a, b).

Some notes:

- $\gcd(0, 0)$ is undefined
- $\gcd(a, 0)$ is equal to $|a|$.
- $\gcd(a, a)$ is $|a|$.

1.1.6 Theorem Let a and b be integers, not both zero. Then a and b have a greatest common divisor, which can be expressed as the smallest positive linear combination of a and b. Moreover, an integer is a linear combination of a and b if and only if it is a multiple of (a, b).

Proof thoughts: Just until I figure out how to label something as an appendix, lets put the definition of a linear combination here: If a and b are integers, we will refer to any integer in the form $ma+nb,\ m, n \in \mathbb{Z}$ as a linear combination of a and b.

So this proof isn't too hard to get when the others are under your belt. First we build a set of all linear combinations of a and b. We want to use the previous theorem to show that every linear combination is a multiple of the smallest gcd in the set. Now, I wrote some python code that shows that this is true for small combinations, but I think this proof makes sense after seeing it a few times. I definitely understand how we got the fact that it was a common divisor, although these proofs are a little suss to me still. But, to show it was the greatest is a little trippy to me because it is a proof by contradiction, which I think is ass. One rabbit hole on Intuitionistic logic, let us get to the proof.

Proof: Let I be the set of all linear combinations of a and b.

$$I = \{x \in \mathbb{Z} | x = ma + nb, \text{ for some } m, n \in \mathbb{Z}\}$$

We would like to use the previous theorem to show that all elements in I are multiples of the smallest linear combination.

First, we will show that I is not empty, and closed under addition and subtraction. It is clear that letting $m = 1,\ n = 0$ that $a \in I$, and $m = 0,\ n = 1,\ b \in I$. So I is not empty.

Second, It is closed under addition and subtraction since for any two $i_0, i_1 \in I, i_0 \pm i_1 = (m_0a + n_0b) \pm (m_1a + n_1b) = a(m_0 \pm m_1) + b(n_0 \pm n_1)$, so $i_0 \pm i_1 \in I$.

By the previous theorem, every element in I, that is, every linear combination, is a multiple of its smallest positive element, $d = m_sa + n_sb$.

We have shown that d is a linear combination of a and b. We will now show that it is a common divisor of both, and then that it is the greatest common divisor.

Claim: $d|a$ and $d|b$. We have shown that every element in I is a multiple of d. Since a and b are in I, $d|a$ and $d|b$.

Claim: If $c|a$ and $c|b$, $c|d$. In other words, any other divisor of a and b divides d, and therefore d is the largest.

If $c|a$ and $c|b$, then $a = k_0c$ and $b = k_1c$. Since $d = m_sa + n_sb, = m_s(k_0c) + n_ss(k_0c) = c(m_s \cdot k_0 + n_ss \cdot k_0c)$. Since d was defined to be a positive integer, it must be greater than or equal to c, and so d is the greatest common divisor.

1.2 Primes

1.2.1 Definition (Relative Primes) Two non zero integers are considered to be relatively prime if $(a, b) = 1$.

1.2.2 Proposition Let a and b be two non-zero integers. Then $(a, b) = 1$ if and only if for some $m, n \in \mathbb{Z}$, $ma + nb = 1$.

Proof thoughts: Not much really, this one is pretty straight forward.

Proof: We will handle the bi-conditional case by case. In the first case, if $(a, b) = 1$, then by Theorem 1.1.6, there do exist m, n such that $ma + nb = 1$.

For the converse, $ma + nb = 1$ implies $(a, b) = 1$, since 1 is the smallest non negative element, and is a linear combination of a and b, then it must be the gcd by Theorem 1.1.6.

1.2.3 Proposition Let $a,\ b,\ c$ be integers, where $a \neq 0$ or $b \neq 0$.

1. If $b|ac$ then $b|(a,b)\cdot c$.

   Proof: Rewrite $(a,b)\cdot c$ as $(ma+nb)\cdot c = mac+nbc$. Since $b|ac,\ ac = kb$ for some $k \in \mathbb{Z}$, so $mac+nbc = mkb+nbc = b(mk+nc)$. so $b|(a,b)\cdot c$.

2. If $b|ac$ and $(a, b = 1)$, then $b|c$.

   Proof: Plug $(a, b = 1)$ into the previous proof.

3. If $b|a,\ c|a$ and $(b,c) = 1$, then $bc|a$.

   Proof: If $b|a,\ a = bq$. If $c|a,\ c|bq$. Since $(b,q) = 1$, then $c|q,\ q = kc$. Therefore $a = bkc = bck$, so $bc|a$.

4. $(a,bc) = 1$ if and only if $(a,b) = 1$ and $(a,c) = 1$.

   Proof by cases: If $(a,bc) = 1$ then $(a,b) = 1$ and $(a,c) = 1$. Since $(a,bc) = 1 = ma + nbc$, we can view this as $ma + (nb)c$ in which case $(a,c) = 1$, or $ma + (nc)b$, in which case $(a,b) = 1$.

   If $(a,b) = 1$ and $(a,c) = 1$ then $(a,bc) = 1$. We see that $(a,c) = 1 = m_1a + n_1c$ and $(a,b) = 1 = m_2a + n_2b$. Multiplying them, $1 \cdot 1 = (m_2a+n_2b) * (m_1a+n_1c) = (m_2m_1a+n_1m_1c+m_2n_1b)a+n_1n_2bc = 1$.

1.3 Congruence

1.3.1 Definition Let a, b, and $n > 0$ be positive integers. Then a and b are said to be **congruent modulo n** if they have same remainder when divided by n. This is denoted $a \equiv b \pmod{n}$.

The division in this case refers to the Division Algorithm, which states that there exists $q\, r \in \mathbb{Z}$ such that $a = q_an + r_a$. Likewise, $b = q_bn + r_b$. Then for $a \equiv b \pmod{n}$, we need $r_a = r_b = r$.

1.3.2 Proposition Let a, b, and $n > 0 \in Integers$. Then $a \equiv b \pmod{n}$ if and only if $n|(a-b)$.

Since we have $a \equiv b \pmod{n}$, by definition a and b have the same remainder r, so we have $a = nq_a = r$ and $b = nq_b + r$. Then

$$a - b = (nq_a + r) - (nq_b + r) = nq_a - nq_b = n(q_a - q_b)$$

and this is divisible by n.

Next we show the converse, if $n|(a-b)$, then $a \equiv b \pmod{n}$. We want to show that a and b have the same remainder. Since we know $n|(a-b)$, there exists a $k \in \mathbb{Z}$ such that $a - b = kn$, so $b = a - kn$. Applying division with respect to n we have $a = nq_a + r$, where $0 \leq r < n$. We know $b = nq_a + r - nk$, so we have $b = n(q_a - k) + r$. Since a and b both have remainder r, where $0 \leq r < n$. So we know that $n|b = r$ as well. Therefore, $a \equiv b \pmod{n}$.

1.3.3 Proposition Let $n > 0 \in \mathbb{Z}$. Then for $a, b, c, d \in \mathbb{Z}$:

(a) If $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$, then $a \pm b \equiv c \pm d \pmod{n}$ and $ab \equiv cd \pmod{n}$.

Proof: We will show this for the positive, without loss of generality for subtraction. Notice that $n|(a-b)$ implies $a - b = nk$ for some $k \in \mathbb{Z}$. Likewise $n|(b-d)$ implies $b - d = nj$. Then it follows that $nj - nk = n(j-k)$ so $n|(a-c) + (b-d)$, so $n|(a+b) - (c+d)$. Therefore $a \pm b \equiv c \pm d \pmod{n}$.

(b) If $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$, then $ab \equiv cd \pmod{n}$:

Since $n|a-c,\ n|(ab-cb)$ and since $n|b-d,\ n|cb-cd$. Adding together we get $n|(ab-cb)-(cb-cd) = n|ab-cb$ and therefore $ab \equiv cd \pmod{n}$.

(c) If $a + c \equiv a + d \pmod{n}$ then $c \equiv d \pmod{n}$.

Proof: Notice that $n|(a+c)-(a+d)$ and $(a+c)-(a+d) = c-d$, so $n|c-d$ therefore $c \equiv d \pmod{n}$.

(d) If $ac \equiv ad \pmod{n}$ and $(a, n) = 1$, then $c \equiv d \pmod{n}$.

Proof: Notice $n|ac - ad$, so $n|a(c-d)$. Since $(a, n) = 1$, then by Prop 1.2.3b, $n|c-d$ and so $c \equiv d \pmod{n}$.

So armed with this knowledge, we get a few useful building blocks.

- You can swap any number in the congruence with a congruent integer $15 \equiv 42 \pmod{3} = 18 \equiv 42 \pmod{3} = 21 \equiv 27 \pmod{3}$.
- You can add or subtract any number from both sides of the congruence.
- You can multiply both sides by the same integer. This one is powerful. $109 \equiv 5 \pmod{8}$ and $39 \equiv 3 \pmod{8}$. Computing

mod base 8 of (109)(39) is a pain, except that it's actually just $5 \cdot 3 \equiv 7 \pmod{8}$.

– You can divide by an integer sometimes. The divisor needs to be relatively prime to the modulus. As an example, $56 \equiv 16 \pmod{8}$, but dividing both sides by 4 we get $14 \equiv 4 \pmod{8}$.

1.4 Congruence Classes

Notes to come when covered in class

Chapter 2

Sets

Notes to come

2.1 Functions

2.2 Equivalence Relations

2.2.1 Definition Let S be a set. A subset R of $S \times S$ is called an equivalence relation of S if it satisfies the following:

1. Reflexive: For all $a \in S$, $(a, a) \in R$.
2. Symmetric: For all $a, b \in S$ $(a, b) \in R$ implies $(b, a) \in R$.
3. Transitive: For all $a, b, c \in S$, if $(a, b) \in R$ and $(a, c) \in R$ implies $(a, c) \in R$.

If $(a, b) \in R$ then we write $a \sim b$.

Chapter 3

Groups

3.1 Binary Operations

Okay, so we are going off-book for some of this, combing what we learned in class with what we see in the assigned textbook.

3.1.1 Definition (Binary Operation) A **Binary Operation** $*$ on a set S is a function $* : S \times S \to S$. That is, a function that takes an ordered pair $a, b \in S$ and maps it to an element $c \in S$.

So we're quite familiar with these. Addition, Multiplication, Modulo, we have tons of examples of things that behave this way, $*(a, b) = c$.

Note that since we write these a whole bunch, rather than using $*(a, b) = c$ (prefix notation for the nerds) we instead use $a * b = c$ (infix notation). Often though, we drop the $*$ altogether: $ab = c$.

3.1.2 Definition (Associativity) The binary operation $*$ is considered associative if $a * (b * c) = (a * b) * c$.

Think of how $a+b+c$, when you include parenthesis, doesn't change its value regardless of how you apply the parenthesis. Not everything is like that. Matrix multiplication is the prime example. Later we learn about how flipping and rotating shapes isn't like that either. Heres a really good one. Check for yourself that $average(average(a, b), c) \neq average(a, average(b, c))$.

3.1.3 Definition (Identities) An element $e \in S$ is called an identity for a

binary operation $*$ if $a * e = a$.

In class, we deal with "left" and "right" identities, which may also be called left and right neutrals. A left neutral e_L is one where $e_L * a = a$. This does not say anything at all about what $a * e_l$ is. We have a similar definition for the right neutral e_R: $a * e_R = a$, and no word on what $e_R * a$ is.

As an example, lets take $* : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ such that $a * b = a^b$. So $2 * 3 = 2^3 = 8$. Well, here we have a right neutral, 1. For any $a \in \mathbb{Z}$, $a * 1 = a^1 = a$. Easy. What we don't have is a left neutral. We cannot say that for all $a \in \mathbb{Z}$ there is a b $b * a = a$. So there isn't a left neutral here, just a right.

3.1.4 Proposition If S has a left neutral and a right neutral with respect to $*$, then they are equal to each other.

Proof: Since for all $a \in S$, $a = e_L * a$ and $a = a * e_R$, then $e_R = e_L * e_R = e_L$.

This one is just a matter of perspective. You can think of $e_L * e_R$ as the left applying itself on the right first, or the right applying itself on the left first, but they are both equally valid, and so we get the equality.

3.1.5 Corollary If S has more than one neutral element e_0, e_1, then there are all equal to each other, and we call them The Identity.

Proof: $e_0 = e_0 e_1 = e_1$.

3.1.6 Definition (Inverses) If $*$ has an identity e, then for any $a \in S$, $b \in S$ is said to be an inverse of a if $a * b = e$ and $b * a = e$.

Our obvious examples here are positive and negative numbers when adding. For our identity, we have 0, since $0 + a = a + 0 = 0$. For our inverse, we have $-a$ since $a + -a = 0$ and $-a + a = 0$.

Notice how we have the same distinction between left and right inverses in the definition though. It doesn't always come up, but it's good to be aware of it. This happens when we lose information in one direction, but not the other.

3.1.7 Proposition If S has a left inverse and a left neutral, then it has a right inverse and right neutral.

See Problem 2.1

3.1.8 Proposition If $*$ is an associative binary operation on S, with an identity, then any element of S has a most one inverse

Proof: Let $b, b' \in S$ be inverses of $a \in S$. Then $a * b = e$ and $b' * a = e$. It follows that $b' = eb' = (ba)b' = b(ab')$ by associativity, and $b(ab') = be = b$.

There are some other things we can prove too, I'll come back to it later.

3.2 Binary Structures

3.2.1 Definition A binary structure is a set S, and a binary operation $*$.

3.2.2 Definition (Magma) A magma is a binary structure $(S, *)$. It isn't particularly interesting for our purposes

3.2.3 Definition (Semigroup) A Semigroup is a magma where the operation is associative. No other requirements are made on it.

While this is also very simple, we get a lot of interesting operations just through semigroups. I'm not gonna go into them here cause we are on a mission.

3.2.4 Definition (Monoid) A Monoid is a semigroup where the operation has an identity element with respect to the set.

3.2.5 Definition (Group) A Group is a Monoid where every element has an inverse.

Chapter 4

Appendix