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. Lets 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 Modulo Congruence

1.4 Congruence Classes

Chapter 2

Sets

2.1 Functions

Chapter 3

Groups

Chapter 4

Appendix