# Lecture 1

This week's material should be review except possibly for sections 0.3 and 1.1. So I am going to supplement only a bit of 0.1 and 0.2. If this material is new to you, you may be in the wrong course or need to do some remedial work ASAP.

The biggest stumbling block for students in section 0.1 is usually the concept of equivalence class. That may be because we are used to thinking of elements as uniquely written, such as $1,\ 3.14159, e$. But actually, we are used to equivalence classes in the rational numbers, *i.e.,* $1/2 = 2/4 = 3/6 = \cdots$.

Proposition 2 is telling for why an equivalence class is set, so I will give a proof omitted by the book.

Suppose $\sim$ is an equivalence relation on a non-empty set $A$ and let $[a]$ be the equivalence class for which $a$ is a representative I claim the equivalence classes form a partition of $A$. Let $a \in A$. Then $a \sim a$, so $a \in [a]$. Thus $\bigcup_{a\in A}[a] = A$. Suppose $c \in [a] \cap [b]$. Then $a \sim c$ and $c \sim b$, whence $a \sim b$. If $d \in [a]$, then $d \sim a$ and $a \sim b$, so $d \sim b$ and $d \in [b]$, whence $[a] \subseteq [b]$. By interchanging the roles of $a$ and $b$, we see that $[b] \subseteq [a]$. Thus $[a] = [b]$. Therefore, the equivalence classes are disjoint and form a partition of $A$.

Conversely, suppose $\{A_i|\ i \in I\}$ is a partition of $A$. Define $a \sim b$ if and only if $a, b \in A_i$ for some $i$. Since the $A_i$ are a partition, each element of $A$ is in one and only one set in the partition. Thus $\sim$ is well-defined and $a \sim a$. If $a \sim b$, then $a, b \in A_i$, so $b, a \in A_i$, whence $b \sim a$. If $a \sim b$ and $b \sim c$, then $a, b \in A_i$ and $b, c \in A_j$. Since $A_i \cap A_j \neq \emptyset$, $i = j$ and $a \sim c$. Thus $\sim$ is an equivalence relation.

The Euler Phi function is likely to be the only new idea in section 0.2. The process to compute it is to first factor the positive integer according to the Fundamental Theorem of Arithmetic and then apply the formula. Here are some other examples.

$95 = 5 \cdot 19$, so $\phi(95) = 5^0(5-1)19^0(19-1) = 4 \cdot 18 = 72$

$96 = 2^5 3$, so $\phi(96) = 2^4(2-1)3^0(3-1) = 2^4 \cdot 2 = 2^5 = 32$.

97 is prime, so $\phi(97) = 96$.

I'm hoping that all of you have seen modular arithmetic and know how to compute in it. Note that the book is using $\overline{a}$ for the class of $a$ which I used as $[a]$ in section 0.1. Both notations are used. I find it easier to type the brackets than put in an overline, but easier to write the overline. Use what works for you but be clear which you are using.

The computations here are awkward. We will learn a shortcut later when we study orders of elements in groups. For the moment, follow the instructions in the book to get a feel for what is going on.

Suppose we are working in $\mathbf{Z}/19\mathbf{Z}$. Then $[(27)^{123}] = [8^{123}] = [2^{369}] = [(2^{18})^{20}2^9] = [2^9] = [64 \cdot 8] = [7 \cdot 8] = [56] = [18] = [-1]$. Yes, this is tedious, but it always works. I tend to stay between $-n/2$ and $n/2$ for my representatives as it makes arithmetic easier. By the way, I did the above computation without a calculator and just picked the numbers at random.

Many of the proofs in modular arithmetic use the Fundamental Theorem of Arithmetic, greatest common divisors and writing them as a linear combination of the number and the modulus (19 in the above example), and so the Euclidean Algorithm.

This week starts group theory. If you've had an abstract algebra course before, much of this is review. If you've not, please work more of the problems, especially the early ones that give you a view of what is and what is not a group or a binary operation.

I'm going to add some theorems that are done in a first course in hopes of helping those of you for whom this is new.

**Theorem 1:** Let $G$ be a group with operation $*$. Then

1. The identity element $e$ is unique.
2. The inverse of a given $x \in G$ is unique.
3. $(a * b)^{-1} = b^{-1} * a^{-1}$ for all $a, b \in G$.

Proof: 1. Suppose $e$ and $e'$ are identities for $G$. The $e = e * e' = e'$.

2. Suppose $b, c$ are both inverses of $a$. Then $b = be = b(ac) = (ba)c = ec = c$.

3. $a*b*(b^{-1}*a^{-1}) = a*(b*b^{-1})*a^{-1} = a*e*a^{-1} = aa^{-1} = e$ Similarly, $(b^{-1}*a^{-1})*a*b = e$. By 2., $(a*b)^{-1} = b^{-1}*a^{-1}$.

**Theorem 2:** $(G, *)$ is a group if and only if

1. The operation $*$ is associative on $G$.
2. There exists a left identity $e$ on $G$, i.e., $e*x = x$ for all $x \in G$.
3. There exists a left inverse $x'$ for each $x \in G$.

Note: The identity and inverse must both be left or both be right but not one of each.

Proof: $x*x' = x*(e*x') = x*(x'*x)*' = (x*x')^2$. Let $y$ be the left inverse of $x*x'$. Then $e = y*(x*x') = y(x*x')^2 = e*(x*x') = e$. Thus $x'$ is a right inverse of $x$ as well. So $x*e = x*(x'*x) = (x*x')*x = e*x = x$. Thus $G$ is a group.

The book alludes to making group tables for finite groups. Let's look and see what this tells us about some small numbered groups. If $G$ has one element, it must be $e$ with $e*e = e$. So suppose $|G| = 2$, so $G = \{e, a\}$. The group table has no choice since $e*x = x = x*e$ fills in three spots. This leaves $a*a$. But $a$ must have an inverse, so $a*a = e$. We get

| * | e | a |
|---|---|---|
| e | e | a |
| a | a | e |

.

Now suppose $|G| = 3$. We start with

| * | e | a | b |
|---|---|---|---|
| e | e | a | b |
| a | a | | |
| b | b | | |

Since $a \neq e$, $a*b \neq b$. Thus $a*b = e$. Since each row and column must have each element once and only once by cancellation, the other three entries are determined:

| * | e | a | b |
|---|---|---|---|
| e | e | a | b |
| a | a | b | e |
| b | b | e | a |

The situation is more complicated for $|G| = 4$ since we can have $a * a = e = b * b = c * c$ or only one of them, say $b * b = e$. We only care about the table up to relabeling, so if $a * a = e = b * b = c * c$,

| * | e | a | b | c |
|---|---|---|---|---|
| e | e | a | b | c |
| a | a | e | c | b |
| b | b | c | e | a |
| c | c | b | a | e |

If $a * a \neq e,\ c * c \neq e$, then

| * | e | a | b | c |
|---|---|---|---|---|
| e | e | a | b | c |
| a | a | b | c | e |
| b | b | c | e | a |
| c | c | e | a | b |

The process becomes more difficult with larger $|G|$, so I will stop here. Please notice that all the groups so far are abelian. Once we have Lagrange's Theorem, we will see that there is exactly one group of order 5, namely, $Z/5Z$. So the first non-abelian group is of order 6, namely $D_6 \cong S_3$. We'll learn about isomorphisms next week and prove this result.

I hope you enjoy working the problems.