Thomas Martinez
Math 61
Some Notes
Winter 2023

These are just some notes that I think are useful to keep in mind. I may add some more notes throughout the quarter for especially confusing topics or if there is enough desire. If there are any questions (or you notice a typo or otherwise), please feel free to email me or come to my office hours and let me know. I am happy to receive any feedback/ideas from this!

# 1 Modular Arithmetic

Modular arithmetic is a concept that we will go over more in depth near the end of the course, but I find it to be useful for you all to gain some idea of what it is right now. That being said, if you don't feel too comfortable with it right now, that is okay. Let us start with define our objects.

$$y \bmod n = x \text{ if } y = nq + x, \text{ for } q \in \mathbb{Z}, 0 \leq x < n.$$

The idea here[1] is the $x$ is the (smallest) remainder of dividing $y$ by $n$. If you remember doing long division in elementary school, it makes a reappearance here.

**Example 1.1.** We have $32 \bmod 3 = 2$ since $32 = 10 \cdot 3 + 2$ and $0 \leq 2 < 3$.

Here is the **full definition (and the definition everyone should become familiar with)** of mod which I think is beneficial for everyone to be familiar with:

$$y \bmod n \equiv x \text{ if } y = nq + x, \text{ for } q \in \mathbb{Z}.$$

What are the differences from this definition and the one above it? In this definition, $=$ is replaced by $\equiv$, and $x$ no longer has a restriction. In plain english, this reads "$y$ mod $n$ is equivalent to $x$". It is worth noting that $\equiv$ does exactly what you would "want" it to do[2], but the nuances are not very important here. Another way to write the above definition is

$$y \equiv x \pmod{n} \text{ if } y - x = nq, \text{ for } q \in \mathbb{Z}.$$

Notice that I moved where I wrote "mod $n$". This is purely a matter of convention. This definition gets to the key idea of mods: two integers $x, y$ are equivalent mod $n$ if there are separated by a multiple of $n$.

**Example 1.2.** We still have $32 \equiv 2 \pmod{3}$ since $32 - 2 = 30 = 10 \cdot 3$.

Additionally, we also have $32 \equiv 35 \pmod{3}$ since $32 - 35 = -3 = (-1) \cdot 3$.

Another fun example is $32 \equiv -1 \pmod{3}$ since $32 - (-1) = 33 = 11 \cdot 3$.

Notice, as well, that since $32 \equiv -1 \pmod{3}$ and $32 \equiv 2 \pmod{3}$, I can also say $-1 \equiv 2 \pmod{3}$.

[1] For those of you in computer science, you may know mod as the % symbol, they do the same thing.

[2] by this, I mean that $\equiv$ is an equivalence relation. Namely, it satisfies the following three properties. For all $a, b, c \in \mathbb{Z}$: (1) $a \equiv a$, (2) if $a \equiv b$ then $b \equiv a$, (3) and if $a \equiv b$ and $b \equiv c$, then $a \equiv c$. Basically, you can treat it like you would the equals sign: $=$.

Now it is important to know what it is you can do with mods. You can take it for granted that we can add, subtract, and multiply. Dividing, however, is not something we can do in general. I'll provide examples of what I mean here.

Not only can I add with mods, but the order doesn't matter. That is, I can add and then take mods, or I can take mods and then add.

**Example 1.3.**

$$1 \equiv 36 = 12 + 24 \equiv 2 + 4 = 6 \pmod 5.$$

The conclusion here is $1 \equiv 6 \pmod 5$ (not $1 = 6$).

**Example 1.4.** Adding doesn't change mods. For example, we have $6 \equiv 18 \pmod 1 2$, and if I add 3, I get $9 = 6 + 3 \equiv 18 + 3 = 21 \pmod 1 2$.

**Example 1.5.** Similarly, multiplying doesn't change mods. For example, we have $5 \equiv 8 \pmod 3$, and if I multiply by 3 I get $15 = 3 * 5 \equiv 3 * 8 = 24 \pmod 3$.

**Example 1.6.** Again, dividing isn't something I can generally do. For example, we have $4 \equiv 8 \pmod 8$, however if I divide by 4, I get $1 = 4/4 \equiv 8/4 = 2 \pmod 2$, which is not true.

We'll end this section with an example problem which uses mods, so you can see their use. Mods are good to use in proofs because they reduce an *infinite* problem to a *finite* one. It is also one of the most common ways to lay out the cases in a "proof by cases" type problem; one of the most common manners is when the two cases are when an integer is odd or even, i.e., when you are working mod 2. The following problem does exactly this.

**Problem:** Do there exist $x, y, z \in \mathbb{Z}$ such that $x^2 + y^2 = 4z + 3$?

*Proof.* No. We prove this assertion. We can rewrite the problem to instead ask if there exist integers $x, y \in \mathbb{Z}$ such that

$$x^2 + y^2 \equiv 3 \pmod 4.$$

In order to answer this, we find the possible values of $x^2 \bmod 4$ for $x \in \mathbb{Z}$.

Case 1: Suppose $x$ is even. Then, $x = 2k$ for some $k \in \mathbb{Z}$, which implies

$$x^2 = (2k)^2 = 4k^2 \equiv 0 \pmod 4.$$

Case 2: Suppose $x$ is odd. Then, $x = 2k + 1$ for some $k \in \mathbb{Z}$, which implies

$$x^2 = (2k + 1)^2 = 4k^2 + 4k + 1 \equiv 1 \pmod 4.$$

So, from these cases, we notice

$$x^2 + y^2 \equiv \begin{cases} 0 & x, y \text{ even}, \\ 1 & x \text{ even}, y \text{ odd, or vice versa}, \\ 2 & x, y \text{ odd}, \end{cases} \pmod 4.$$

From this, we see that it is impossible for $x^2 + y^2 \equiv 3 \pmod 4$, thus proving our assertion. □

## 2 An Induction Proof

What I want to go over here is a (more complicated) proof by induction. This proof was discussed quickly in class, and the overall proof is not particularly important (i.e. you won't need to memorize this), but it demonstrates a lot of components in a nice package.

Before we begin, let us illustrate the key idea of the inductive step. For any (nonempty) set $X$ pick some $x \in X$. Then, we can partition $P(X)$ into two kinds of subsets of $X$: the ones which contain $x$ and the ones that don't contain $x$. Notice that this covers every case, since every set can either contain $x$ or not. It turns out, however, that these two sets are **of the same size**. That is, the number of subsets which contain $x$ are the same as the number of subsets which do not contain $x$. Let us illustrate this with an example.

Let $X = \{a, b, c\}$. Then,

$$P(X) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

Let me write this more... suggestively.

$$\begin{aligned} \emptyset &\leftrightarrow \{a\} \\ \{b\} &\leftrightarrow \{a, b\} \\ \{c\} &\leftrightarrow \{a, c\} \\ \{b, c\} &\leftrightarrow \{a, b, c\} \end{aligned}$$

As you can see, the sets on the left hand side do not contain $a$, and the sets on the right hand side all contain $a$. There are 4 of each, and more importantly, I can pair these sets up in a nice way. This is what the function $f$ is doing in the induction proof below, just in a more abstract sense.

**Problem:** Prove that if $|X| = n$, then $|P(X)| = 2^n$ for $n \in \mathbb{N}_0$.

*Proof.* **Base Case.** When $n = 0$, that implies $X = \emptyset$. So, $P(\emptyset) = \{\emptyset\}$, implying $|P(X)| = 1 = 2^0$.

**Inductive Hypothesis.** Suppose that, for some $n \in \mathbb{N}_0$, if $|X| = n$ then $|P(X)| = 2^n$.

**Inductive Step.** Let $|Y| = n + 1$, and let $y \in Y$ be given. We know such $y$ exists as $n + 1 \geq 1$. Let $X = Y - \{y\}$. Then,

$$Y = X \cup \{y\} \quad \text{and} \quad |X| = |Y| - |\{y\}| = n + 1 - 1 = n.$$

By the **inductive hypothesis**, we have that $|P(X)| = 2^n$. We also know that we can *partition* $P(Y)$ in the following manner:

$$P(Y) = \{S \mid S \subseteq Y\} = \{S \mid S \subseteq Y, y \in S\} \cup \{S \mid S \subseteq Y, y \notin S\}.$$

Notice, however, that since $y \notin X$,

$$P(X) = \{S \mid S \subseteq X\} = \{S \mid S \subseteq Y - \{y\}\} = \{S \mid S \subseteq Y, y \notin S\}.$$

So, via we find

$$\begin{aligned} |P(Y)| &= |\{S \mid S \subseteq Y, y \in S\}| + |\{S \mid S \subseteq Y, y \notin S\}| \\ &= |\{S \mid S \subseteq Y, y \in S\}| + |P(X)| \end{aligned}$$

$$= |\{S \mid S \subseteq Y, y \in S\}| + 2^n.$$

So, letting $A = \{S \mid S \subseteq Y, y \in S\}$, if we can create a bijection $f : P(X) \to A$, then, $|A| = |P(X)| = 2^n$. Let

$$\begin{aligned} f\colon P(X) &\to A \\ S &\mapsto S \cup \{y\}. \end{aligned}$$

We first show $f$ is injective. Suppose that $S_1 \cup \{y\} = f(S_1) = f(S_2) = S_2 \cup \{y\}$. Then, since $y \notin S_1$, we have that

$$(S_1 \cup \{y\}) - \{y\} = S_1.$$

Similarly, we obtain $(S_2 \cup \{y\}) - \{y\} = S_2$. Thus,

$$S_1 = (S_1 \cup \{y\}) - \{y\} = (S_2 \cup \{y\}) - \{y\} = S_2,$$

implying $f$ is injective. We now show $f$ is surjective. Let $S \in A = \{S \mid S \subseteq Y, y \in S\}$ be given. Then, $y \in S$ and we can write $S = T \cup \{y\}$ where $T \subseteq Y$ and $y \notin S$. That is, $T \subseteq X$. Thus, $f(T) = T \cup \{y\} = S$, implying $f$ is surjective.

Thus, $f$ is bijective and we obtain $|A| = |P(X) = 2^n$, giving

$$|P(Y)| = |A| + |P(X)| = 2^n + 2^n = 2\,2^n = 2^{n+1},$$

completing the proof. □

If you've made it this far, you'll notice that this proof is... long to say the least. We have to be clever with rewriting $P(Y)$ in order to use the inductive hypothesis, and then create a bijection to work things out. As it turns out, when we get introduced to combinatorics, we can actually do a different, simpler, proof (which has a total length of 4 lines).