Modular Arithmetic and Congruences

Reading

- Section 7.1

Practice Problems

7.1 2, 4, 7, 8, 10
Challenge 7.1 (Optional) 9, 16, 18, 19, 20, 21, 28

Notes

Modular arithmetic considers operations "up to a multiple of a specific number". That specific number is called the **modulus**.

You are rather used to this already: If it is now 11 o'clock, then 2 hours later it will be 1 o'clock, and not 13. This is because we "reset things" every time we hit 12. This is really the same as saying: We ignore multiples of 12 in "clock arithmetic".

Let us start with our key definition:

> We say a, b are **congruent modulo n**, if $n|(a-b)$, in other words if they differ by a multiple of n.
>
> n is called the **modulus** in this case.
>
> We write: $a \equiv b \bmod n$

$$a \equiv b \bmod n \iff n|(a-b) \iff a = b + kn \quad \text{for some } k \in \mathbb{Z}$$

For instance, "modulo 4", the numbers 1, 5, 9, 13 are all congruent to each other. In fact every number that leaves a remainder of 1 when divided by 4 is congruent to them as well.

Food for thought: When are two numbers congruent modulo 2?

In fact, the consideration of the remainder is the only condition for two numbers to be congruent:

> a, b are congruent modulo n if and only if they leave the same remainder when divided by n.
>
> We often call this remainder the **reduction of a modulo n**.
>
> If r is the reduction of a modulo n, then we have:
>
> - $a \equiv r \bmod n$

- r is one of $0, 1, \ldots, n-1$

The later parts follow easily from the first. Let us show the first part:

- Say $a = q_1 n + r_1$, $b = q_2 n + r_2$, with $0 \leq r_1, r_2 < n$.
- Then $a - b = (q_1 - q_2)n + (r_1 - r_2)$.
- So $n|(a-b)$ if and only if $n|(r_1 - r_2)$.
- But since $-n < r_1 - r_2 < n$, this happens iff $r_1 - r_2 = 0$.

A key property of congruence is that **congruence is an equivalence relation**:

1. $a \equiv a \bmod n$ for all a.
2. If $a \equiv b \bmod n$ then we also have $b \equiv a \bmod n$.
3. If $a \equiv b \bmod n$ and $b \equiv c \bmod n$, then it is also the case that $a \equiv c \bmod n$.

These are all easy to see and left as exercise for the reader.

If you are familiar with equivalences, then the following should be easy to follow. If not, we will go into greater detail in the next section:

Whenever you have an equivalence, your set in decomposed into *equivalence classes*: These are disjoint sets, each consisting of all elements that are equivalent to each other. Every element is in one equivalence class.

In the case of congruences, we call these **congruence classes**:

- Two numbers a, b are in the same congruence class if and only if they are congruent mod n.
- There are exactly n congruence classes mod n, represented by the possible remainders when divided by n.
- The congruence class corresponding to the remainder r can be described as $\{r + kn \mid k \in \mathbb{Z}\}$.

More on equivalences

We will assume in this section that you are not too familiar with equivalences, and we will build things from the ground up. First off, let's recall the 3 key properties that make congruence an equivalence:

1. (reflexivity) $a \equiv a \bmod n$ for all a.
2. (symmetry) If $a \equiv b \bmod n$ then we also have $b \equiv a \bmod n$.
3. (transitivity) If $a \equiv b \bmod n$ and $b \equiv c \bmod n$, then it is also the case that $a \equiv c \bmod n$.

Armed with this in hand, let us make the following definition:

The *congruence class of* a is the set of all b that are congruent to a. In other words it is the set:

$$C(a) = \{a + nk \mid k \in \mathbb{Z}\} = \{b \mid b \equiv a \bmod n\}$$

We will show the following:

1. For all a, the set $C(a)$ is non-empty.
2. For any a, b, we have $a \equiv b \bmod n$ if and only if $C(a) = C(b)$ if and only if $b \in C(a)$.
3. If $a \not\equiv b \bmod n$ then $C(a) \cap C(b) = \emptyset$.
4. In other words, the $C(a)$ are disjoint sets, when they are not identical sets.
5. If r is the remainder of dividing a by n, then $a \equiv r \bmod n$ and $C(a) = C(r)$.
6. If $0 \leq r_1 \neq r_2 < n$, then $C(r_1) \neq C(r_2)$.
7. There is exactly one congruence class for each remainder $0, 1, \ldots, n-1$. Every other congruence class is equal to one of these.

Now let us prove each step at a time:

1. $a \in C(a)$ because $a \equiv a \bmod n$. So $C(a)$ is non-empty and containing a.
2. The second statement is the most complicated to show, but it is also the most important one. It has multiple parts, so let's get started:
   - If $a \equiv b \bmod n$, then $C(a) = C(b)$. To show this:
     - First, note that, because of symmetry we also have $b \equiv a \bmod n$.
     - So if we can come up with an argument that $C(a) \subset C(b)$, then the other inclusion will follow by the same reasoning with a and b reversed, and would finish the proof of this part.
     - To show that $C(a) \subset C(b)$, start with a $c \in C(a)$. Then $c \equiv a \bmod n$.
     - Since we also know $a \equiv b \bmod n$, the transitivity property says that $c \equiv b \bmod n$.
     - This is the definition of saying $c \in C(b)$. So we just showed that every element of $C(a)$ is also in $C(b)$.
   - If $C(a) = C(b)$ then $b \in C(a)$. This is trivial, since $b \in C(b)$.
   - If $b \in C(a)$ then $b \equiv a \bmod n$. This follows directly from symmetry. This completes a circular chain of implications.
3. To show that if $a \not\equiv b \bmod n$ then $C(a) \cap C(b) = \emptyset$, we instead show the contrapositive: "If there is a $c \in C(a) \cap C(b)$, then it must be the case that a and b are congruent to each other. To see this:
   - Suppose there was a $c \in C(a)$ and $c \in C(b)$.
   - Then $C(a) = C(c)$ and $C(b) = C(c)$ from the previous part.
   - Therefore $C(a) = C(b)$ which in particular means that a and b are congruent to each other.

4. This follows directly from the previous two parts.
5. Follows directly from the division theorem.
6. This follows because $r_1 - r_2$ cannot be divisible by n without the two remainders being equal to each other.