Lecture 10 notes

Puzzler (last chance at this one):

Last time, Alice and Bob wanted to exchange messages, but the only time they met was in a class where Carl sat between them. Everything they exchanged had to go through Carl. To prevent him from reading their notes, they devised a scheme of using both of their locks on the outside of the suitcase.

But a problem happened: To all appearances, the locks seem identical. In other words, Alice can't see whether or not a lock on the suitcase is really Bob's. She suspects that Carl has been switching suitcases, and the locks that she assumed were Bob's were actually Carl's! It looks like some of the notes she received weren't actually from Bob, but maybe from Carl instead!

This time we're changing the problem a bit: All the locks are now combination locks. Anyone can buy as many combination locks as they want. There is also a blackboard in front of the room, and if anyone wants, they can share the combination to any of their locks if they want.

This time, two kinds of briefcases are available: the regular ones from before, and new smaller ones that can fit inside the regular briefcases. What can Bob and Alice work out (with Carl possibly hearing the whole plan) so that Bob can send a private message to Alice, and Alice can be sure the message came from Bob?

Modular Arithmetic Fundamentals

Part 1 : language and its reconceptualization

$[a]_d$ means the type of number such that when divided by d has the same remainder as a does.

Examples:

- 1 is a number of type $[1]_2$ it is also a number of type $[6]_5$.
- 21 is also a number of type $[6]_5$.
- $[8]_7$, $[1]_7$, $[15]_7$ and $[-6]_7$ are all symbols which represent the same type of number, and 22 is an example of a number of this type (as are 8, 1, 15, and -6).

These types are called congruence classes modulo d. So, for example

- $[1]_2$ is a congruence class modulo 2. It is also the type of number which we call "odd."
- The numbers 8 and 22 are in the same congruence class modulo 7. This congruence class can be denoted by $[1]_7$ or by any of the names from the corresponding example above.

We have another notation for congruence classes: if a and b are in the same congruence class modulo d, we write $a \equiv b \pmod{d}$. We say in this case that a and b are congruent modulo d.

Examples:

- Some numbers which are congruent to 4 modulo 9 are 13, 22, 31.
- Write down some numbers which are congruent to 7 modulo 13

Let's be a bit more formal. What does "type" of number really mean? We have to be careful when using words like this — it feels like we are making up words if we aren't careful, and when we are making up new words, we risk manipulating concepts in ways which are not well grounded or justified. These new words can be very helpful (perhaps essential in a practical sense) for giving us the intuition for working with things conceptually, but at the end of the day, they need to be presented in terms which are grounded in concepts which are already "vetted."

So: what is a "type" of number in this context? It is just a subset of the integers in this case.

In other words, what does being an even number mean? It means being in the subset

$$\{\ldots,-4,-2,0,2,4,\ldots\} = \{2m \mid m \in \mathbb{Z}\} = \{n \in \mathbb{Z} \mid n \text{ is divisible by } 2\}$$

of the integers $\mathbb{Z}$.

In other words, we can define formally $[0]_2 = \{n \in \mathbb{Z} \mid n \text{ is divisible by } 2\}$ and more generally $[a]_d = \{n \in \mathbb{Z} \mid$
$n \text{ has the same remainder that } a \text{ does when divided by } d\}$

so:

- $[3]_7 = \{\ldots, 3, 10, 17\}$

Part 2: Describing congruence classes

Proposition:

Suppose we have integers a, b, d with $d > 0$. Then the following statements are equivalent:

1. $[a]_d = [b]_d$
2. a is in the congruence class $[b]_d$
3. b is in the congruence class $[a]_d$
4. $a - b$ is divisible by d

Before we do this, let's make an initial baby proof:

Lemma:

Suppose a, d are integers with $d > 0$. Then a is in the congruence class $[a]_d$.

proof of the lemma:

a being in the congruence class of a means that a and a have the same remainder when divided by d. Check.

proof of the proposition:

We will show that if 1 is true then 2 is true and if 2 is true then 3 is true and if 3 is true then 4 is true and if 4 is true then 1 is true.

So, suppose that 1 is true. In other words, suppose that the congruence classes of a and b coincide. Since a is in the congruence class $[a]_d$ by the lemma and $[a]_d = [b]_d$ by the hypothesis, it follows that a is in the congruence class of $[b]_d$. Therefore 2 is true.

Now suppose 2 is true. By definition, a is in the congruence class $[b]_d$ means that a and b have the same remainder when divided by d. But this means, also by definition that b is in the congruence class $[a]_d$. Therefore 3 is true.

Now suppose 3 is true. As we said above, this means that a and b have the same remainder when divided by d. By the division algorithm, we can then write $a = qd + r$ and $b = q'd + r$ (notice the same r. But therefore when we subtract, we see that

$a - b = qd + r - q'd - r = (q - q')d$ is a multiple of d

therefore 4 is true.

Now suppose that 4 is true. In other words, suppose that $a - b$ is a multiple of d. We need to show that the sets $[a]_d$ and $[b]_d$ are the same. In other words, we need to show that they have the same elements, or, in other words, that an integer m is in $[a]_d$ if and only if it is in $[b]_d$.

So for example, suppose m is in $[a]_d$. We will show it's in $[b]_d$. Since it is in $[a]_d$ we know that we can write $m = qd + r$ and $a = q'd + r$. Let's suppose that $b = pd + s$. To know that $m \in [b]_d$ we need to show that $s = r$. We can see that $m - a = (q - q')d$ is a multiple of d. We also know that $a - b$ is a multiple of d by assumption. Let's say $a - b = dt$. Then we have $m - b = m - a + a - b = (q - q')d + dt = (q - q' + t)d$ is a multiple of d. But examining the above expressions then gives:

$m - b = qd + r - pd - s = (q - p)d + (r - s)$ is a multiple of d. Copying down, we have actually

$(q - q' + t)d = m - b = (q - p)d + (r - s)$

but therefore we find (subtracting off) that

$(q - q' + t - q + p)d = (t + p - q')d = r - s$ and so $r - s$ is a multiple of d. Of course, by taking negatives, we would also know that $s - r$ is a multiple of d. Let's choose the one which is positive. So for example, if $r \geq s$ we find that $r - s$ is positive and a multiple of d. But look: by the division algorithm, both r and s are strictly less than d. So r is less than d and subtracting off a nonnegative number less than r we find that again $0 \leq r - s < d$. But since $r - s$ is a multiple of d the only possibility is that it is 0. Therefore $r = s$ and m and b have the same remainder when divided by d. Therefore

$m \in [a]_d$ implies $m \in [b]_d$. The argument showing the opposite is exactly the same but with a and b reversed. Therefore $[a]_d = [b]_d$ and 1 is true.

This completes the proof.

This gives us a pretty concrete description of these classes. We find

$[a]_d = \{n \in \mathbb{Z} \mid n - a \text{ is a multiple of } d\} = \{a + md \mid m \in \mathbb{Z}\}$

$= \{\ldots, a - 3d, a - 2d, a - d, a, a + d, a + 2d, \ldots\}$

- list 3 negative integers which are congruent to 2 modulo 14

Recall also the alternate notation:

- $a \equiv b \pmod{d}$ means that a and b are in the same congruence class modulo d

equivalently this means $a - b$ is a multiple of d or that $[a]_d = [b]_d$, for example, by the above.

Part 3: Arithmetic of congruence classes (modular arithmetic)

The punchline: addition, subtraction, multiplication is compatible with types.

In other words: If a and a' are congruent modulo i.e.

$a \equiv a\text{'} \pmod{d}\, d$

and b and b' are congruent modulo d i.e.

$b \equiv b\text{'} \pmod{d}$

then:

- $a + b \equiv a\text{'} + b\text{'} \pmod{d}$

- $a - b \equiv a' - b' \pmod{d}$
- $a \cdot b \equiv a' \cdot b' \pmod{d}$

and for any positive integer n,

- $a^n \equiv (a')^n \pmod{d}$

We can think of this as saying that “arithmetic on types makes sense”

That is: if you have a number of type $[a]_d$ and a number of type $[b]_d$ and you multiply them, you get a number of type $[ab]_d$.

This is what the above says: if we choose a' a number of type $[a]_d$ and we choose b' a number of type $[b]_d$ and we multiply them to get $a'b'$, this is a number of type $[ab]_d$

Divisibility Rules and Games

What about 4? This is a little more complicated, but we can notice that $4|100$ so only need to consider the last two digits. Further, since $[10]_4 = 2$ we can state that a rule could be: a number is a multiple of 4 if the last two digits are. And a 2 digit number is divisible by 4 if twice the first plus the second digit is divisible by 4. So, for example:

to check 291172 we need to check 72 and for this we need to look at $14 + 2 = 16$ so yes.

to check 1892419081252 we check 52 and this gives 12 which is divisible.

to check 214974 we check 74 which reduces to 18 which reduces to 10 which reduces to 2. So no.

Notice in these, we aren’t just checking if a number is divisible by 4, we are also computing its remainder after division!

We can do a similar rule for 8 using the last 3 digits (homework?)

How about 7? For this, there is a really cute trick.

Let's notice that $[10]_7 = [3]_7$ and that $[5]_7[3]_7 = [1]_7$.

As a preamble let's make an observation:

we have $[n]_7 = [0]_7$ if and only if $[5n]_7 = [0]_7$.

So in other words, we can always multiply by 5 without messing our problem up.

Why is this and why is it useful?

Why is it? On the one hand, if $[n]_7 = [0]_7$ then $[5n]_7 = [5]_7[n]_7 = [5]_7[0]_7 = [0]_7$. On the other hand, if $[5n]_7 = 0$ then $[0]_7 = [3]_7[5n]_7 = [3]_7[5]_7[n]_7 = [15]_7[n]_7 = [1]_7[n]_7 = [n]_7$.

Why does it help? The trick.

Now for the trick:

Suppose we have a number with last digit a, so it looks like $n = a + 10b$. Then we have $[n]_7 = 0$ if and only if $[5n]_7 = 0$. But $[5n]_7 = [5a]_7 + [5]_7[10]_7[b]_7 = [5a]_7 + [5]_7[3]_7[b]_7 = [5a + b]_7$.

So, we can check if a number is divisible by 7 by sliding the digits over and adding 5 times the last digit. For example:

To check if 12981 is divisible by 7, we find it is divisible if and only if $1298 + 5 = 1303$ is. And this is if and only if $130 + 15 = 145$ is. And this is if and only if $14 + 25 = 39$ is. And this isn't because it is 4 more than 35.

But this doesn't mean that the remainder of 12981 is 4 when divided by 7. The remainder is actually 3, which we can see by examining 12978

$12978 \to 1297 + 40 = 1337 \to 133 + 35 = 168 \to 16 + 40 = 56 \to 5 + 30 = 35$ is divisible by 7.

We could have actually made a slightly easier rule by using the intuition of the 11 rule above. Notice that $[5]_7 = [-2]_7$. So we could have also said $[a + 10b]_7 = [b - 2a]_7$.

So for example, we would get $891724 \to 89172 - 8 = 89164 \to 8916 - 8 = 8908 \to 890 + 40 = 930 \to 93 \to 9 - 6 = 3$ done. so it is not a multiple of 7. Notice we switched rules in the middle — they both work!!