SRQR: Congruences (April 6, 2021)

> I’ve seen modulo arithmetic before, where a congruent b mod n when the remainder of a/n and b/n are the same. But I’m having a hard time connecting that to the formal definition, that $a - b = kn$.

> When I was doing the Comprehension Check, I found that I still treated this new concept of congruence as the divisor and remainder thing we learned in the previous chapter. (for example, I have to repeat to myself “$a \equiv b \pmod{n}$’’ means $a = b + kn$" when I see this new notation) So, I was wondering how is this different from the divisor thing we learned before, and are there other any ways for me to think about this?

There are in fact these two equivalent ways of thinking about congruence: (1) both numbers have the same remainder when divided by the modulus, or (2) the difference of the two numbers is a multiple of the modulus.

These two versions are entirely equivalent, and this is the statement of theorem 4.1 in the book. I encourage you to work through that proof using a few concrete examples; that should convince yourself that the two definitions are actually the same.

I think version (1) (ie, the “same remainder’’ version) is useful for intuively understanding what congruence means, probably because we’ve all seen quotients and remainders for a long time. It’s also occasionally useful in proofs, but my experience is that version (2) is useful in proofs more often. In other words, proofs involving congruences often (but not always!) end up more efficient if you use version (2) rather than version (1). I expect that is the reason why the definition of congruence in the book is made using version (2).

> I don’t quite get the idea of the “complete set of residues modulo n.”

The formal definition of “complete set of residues modulo n” is on p. 64, so maybe it’s best to consider some examples in detail. Let’s take $n = 5$. Then $S_1 = \{0, 1, 2, 3, 4\}$ is a complete set of residues mod 5, since any number I might pick must be congruent to one of the elements of S mod 5. For example, if I pick 137, it is congruent to 2 mod 5 since $137 - 2 = 135$ is divisible by 5, and 2 is an element of S_1. If I pick 1231, it is congruent to 1 mod 5 since $1231 - 1 = 1230$ is divisible by 5, and 1 is also an element of S_1.

But the set $S_2 = \{0, 11, 7, 23, 14\}$ is also a complete set of residues mod 5, again since any number I might pick must be congruent to one of those mod 5. If I pick 137, it is congruent to 7 mod 5 since $137 - 7 = 130$ is divisible by 5, and 7 is in S_2. If I picked 1231, it is congruent to 11 mod 5 since $1231 - 11 = 1220$ is divisible by 5, and 11 is in S_2.

The set $S_3 = \{0, 11, 7, 14\}$, however, is *not* a complete set of residues mod 5. There are numbers I can pick which are not congruent to any of the numbers in S_3. For example, if I were to pick the number 33, it is not congruent to any of the numbers in S_3:

$$\begin{aligned}
33 - 0 = 33 &\text{ is not divisible by } 5\\
33 - 11 = 22 &\text{ is not divisible by } 5\\
33 - 7 = 26 &\text{ is not divisible by } 5\\
33 - 14 = 19 &\text{ is not divisible by } 5
\end{aligned}$$

As you can see, there can be many different complete sets of residues mod 5. Among all of these, the set $S_1 = \{0, 1, 2, 3, 4\}$ that we considered is special; it goes by the name “the set of the least non-negative residues mod 5.” It’s special because its elements are the remainders we can get when we apply the divison algorithm. It’s the easiest complete set of residues mod 5 to work with.

> It is kind of hard for me to understand this sentence in example 4.3: “The observation that starts us off is that”$4! = 24 \equiv 0 \bmod 12$." Why do we start here?

> Could you explain example 4.3 in section 4.2? It seems kind of random to me that they chose 4! to start off with.

> I don’t get why in example 4.3 the remainder is 9.

You don’t have to start with 4!. In fact, if I were doing this problem, I would start from the bottom and just start computing. I would see that

$$\begin{aligned}
&1! = 1 \equiv 1 \bmod 12\\
&2! = 2 \cdot 1! \equiv 2 \cdot 1 = 2 \bmod 12\\
&3! = 3 \cdot 2! \equiv 3 \cdot 2 = 6 \bmod 12\\
&4! = 4 \cdot 3! \equiv 4 \cdot 6 \equiv 0 \bmod 12\\
&5! = 5 \cdot 4! \equiv 5 \cdot 0 = 0 \bmod 12\\
&6! = 6 \cdot 5! \equiv 6 \cdot 0 = 0 \bmod 12\\
&\quad\vdots
\end{aligned}$$

Notice that once I hit a factorial that’s congruent to 0, all the subsequent factorials are also 0. That means that, mod 12, all of the summands starting from 4! don’t contribute anything! In other words,

$$1! + 2! + \cdots + 100! \equiv 1! + 2! + 3! = 1 + 2 + 6 = 9 \bmod 12.$$