MTH 350 Weekly Practice 2 Due: 11:59pm ET Sunday, 31 January

Directions:

- Complete the exercises below and either write up or type up your solutions. Solutions must be submitted as PDF or Word documents, uploaded to the appropriate assignment area on Blackboard.
- If you choose to submit handwritten work, it must be neat and legible; if you do your handwritten work on paper, it must be **scanned to a PDF file** and submitted to Blackboard. Instructions and practice for scanning work to PDFs is given in the Startup Assignment. **Do not just take a picture**, **and do not submit a graphics file (JPG**, **PNG**, **etc.)** — such submissions will not be graded.
- Your work will be graded using the EMPX rubric and evaluated **not just on the basis of a right or wrong answer**, **but on the quality**, **completeness**, **and clarity of your work**. Therefore you need to show all work and explain your reasoning on each item.
- Every item must have a good-faith effort at a complete and correct response. If any item is left blank, or shows minimal effort (such as answering "I don't know"), or is significantly incomplete, the entire assignment will be graded "X" (Not Assessable) and you will have to spend a token to revise it.

---

1. In class, we looked at a proof of the *existence* part of the Division Algorithm. Let's now do the *uniqueness* part. As a reminder: We have already proven that given two integers a, b with $a > 0$, there exist integers q, r such that $b = aq + r$ and $0 \leq r < a$. We now are trying to show that these two integers are the *only* integers that satisfy both the equation *and* the inequality.

   Below is a proof of the uniqueness of q and r in the Division Algorithm, remixed from the fill-in-the-blanks proof in the book so it's done line by line. We are using the same assumptions and notation as found in the existence part of the proof. For each line, provide a correct justification. Justifications, as always, can come from axioms, previously-proven results (including Activities), or computations.

   > We have found integers q and r such that $b = aq + r$ and $0 \leq r < a$. Suppose that q' and r' are two integers such that $b = aq' + r'$ and $0 \leq r' < a$. We want to show that $r = r'$ and $q = q'$.
   >
   > (a) Given all this information, we can conclude that $a(q - q') = (r' - r)$.
   >
   > (b) We know that $0 \leq r' < a$.
   >
   > (c) We also have that $-a < r \leq 0$.
   >
   > (d) Therefore $-a < r' - r$ and $r' - r < a$. (Justify both claims.)
   >
   > (e) Notice that $r' - r$ is an integer multiple of a (this follows from the first line above) and is strictly between $-a$ and a. Therefore $r' - r = 0$.
   >
   > (f) Therefore $q - q' = 0$.
   >
   > (g) And therefore $r = r'$ and $q = q'$.

2. Integer congruence is the basic mathematical concept behind many forms of **data encryption**, which refers to processes that prevent text or electronic data from being read or copied by anyone but the intended recipient. For example, your Blackboard gradebook data are encrypted using (among other things) a system called RSA, which is rooted in many of the concepts we'll be studying in the early modules of MTH 350.

   Here is a *very* simple encryption method used during the time of the Roman Empire. (In fact it often goes by the name of the *Caesar cipher*.) Suppose Alice wants to send a message to Bob that consists of plain English letters (all upper-case to keep things simple) and no punctuation or numbers. Alice and Bob first agree upon a positive integer they denote K, called the **key**. Then:

- Alice takes her message, strips out all the spaces, and then converts each character to a number representing its position in the alphabet: A is changed to 0, B to 1, and so on, down to Y = 24, Z = 25.
- For each of these "letters" x (which are now numbers between 0 and 25, inclusive) Alice computes $x + K$, and then finds *the smallest positive integer to which $x + K$ is congruent mod 26.* For example if the current letter is R and the key is $K = 11$, Alice would convert R to 17; then compute $17 + 11 = 28$; then reduce this mod 26 to get 2. (This is basically dividing by 26 and keeping the remainder.)
- Alice carries out that process for each letter in the message. Each number that results is between 0 and 25, inclusive; she then converts them all back to letters. This string of letters is the secret message, and she sends it to Bob.
- Bob takes the secret message, converts each letter to a number (A = 0, B = 1, ... , Z = 25) and then for each number y, he computes $z = y - K$ where K is the key. This produces a list of numbers, some possibly negative; Bob then finds the smallest positive integer to which $y - K$ is congruent mod 26. For example, if Bob receives the letter E in the message, he converts this to the number 4, then computes $4 - 11 = -7$ and then "reduces" that mod 26 to get 19.
- The result is a string of integers between 0 and 25, so Bob converts each one back to a letter.

The result is the original message!

(a) Encrypt the message `MATH IS COOL` using this system and a key of 20. Be sure to show your steps.

(b) You've received the following message that was encrypted using this system and a key of 12: `YKOMFEMDQZUOQ`. Find the original message. (It won't have spaces but it will be a real English sentence.)

(c) Why does this system work? That is, what aspect(s) of the mathematics involved will guarantee that Bob always ends up with the correct English message (assuming neither he nor Alice made a mistake)?

(d) Suppose you are Eve, the evil eavesdropper, and you've intercepted this message between Alice and Bob: `QHQEGOWE`. However, you don't know what key was used to encrypt it. What are some possible ways that you could break this code and find the original message? (Bonus points[1] if you can actually recover the original message.)

3. On each Weekly Practice, you'll be asked to reflect on your work for the week and share what you've learned. We'll typically do this by video, using the app **Flipgrid**. Go here: https://flipgrid.com/fe1f98d5 and sign in with your GVSU email credentials, then give a 3-minute (or less) video response to the three prompts that are given. **Note**: **This is a different link than last week**.

[1] Just kidding, there are no points in MTH 350.