# MTH 225: Discrete Structures for Computer Science 1

## Daily Preparation, Module 2A: Modular arithmetic and applications to cryptography

**Due by:** 11:59pm ET, Sunday, September 13

**Estimated time requirement:** About 45-60 minutes for the whole assignment. *If you have worked on this assignment for 30 minutes and you're not at least halfway done, DON'T work any further* — instead, *stop and ask for help* on the `#dailyprep` channel on CampusWire. Remember these are graded just on completeness and effort — try to be right and understand everything, but don't get bogged down if you get stuck. Just give a good effort and move on, and ask a question.

## Overview

In Module 2 we will look at more basic computer arithmetic, this time focusing on a special operation that doesn't have an analogue in our usual school math background: the "modulus" or `%` operator. Like the basic arithmetic operations of adding, subtracting, multiplying, and dividing, the modulus operator takes two numbers as input and produces a third one as an output — but it does it in a special way using the **Division Algorithm** (something we *did* learn in elementary school) and returning a remainder after division. This operation turns out to have profound applications throughout computer science, and we'll take a look at one such application in **cryptography**, the science of making and breaking coded messages. (Shout-out to all the Cybersecurity majors.)

## What you will learn

**Learning Targets addressed in this module:**

- A.3: I can compute `a % b` given integers `a` and `b` and perform modular arithmetic.

**BEFORE** your class meeting, use the Resources for Learning (below) to learn how to do the following:

- State the Division Algorithm and explain its notation and main points.
- Given two integers a, n with n > 0, find `a % n`.
- Encrypt and decrypt using the shift cipher given the key.

**DURING AND AFTER** your class meeting, you will learn how to do the following:

- Compute `a % b` if `a` is a negative integer.
- Encrypt and decrypt using the multiplicative cipher.

## Resources for Learning

**Text:** There's no assigned text to read this time; the videos do it all. However, as always, Google searches will turn up a *lot* of material on the web in case you are needing more help.

**Video:** Watch the following videos. The total running time is 18:35.

- The Division Algorithm (6:51) https://www.youtube.com/watch?v=XHjSy_MT7u0 This was created by me for the class MTH 210, but it also works for MTH 225.
- The modulus operator (1:07) https://www.youtube.com/watch?v=MrTtsX2Wg9Q This video just introduces notation – it does not go into any depth. That's what the next video does:
- The modulus operator (10:37) This video was made by me (Talbert) and can be found in the Module 2 folder.

You are free to search for and use other resources in addition to, or instead of the above, as long as you can work the exercises below.

**Bonus material:** This page has some nice computer science applications of the modulus operator that you may find handy, along with links to additional explanations: https://blog.mattclemente.com/2019/07/12/modulus-operator-modulo-operation.html

## Exercises

The exercises for this assignment are found at Classkick this time. Go to http://app.classkick.com and sign in (as a "Portfolio" student). If prompted, use the code Q4L W99.

## Submission, grading, and getting help

**Submitting your work:** Your work is to be done on Classkick using the link/code above. Classkick saves your work as you go, so there's nothing to submit – just do the work and you're good.

**How this is graded:** Daily Prep assignments are graded on the basis of *completeness and effort*: If your submission has **all parts completed** (no blank entries, even if left blank accidentally) and **a good-faith effort to provide a correct solution or explanation is given** (no responses of "I don't know" or "I didn't understand") and **the work is submitted on time**, it gets a "check". Otherwise it gets an "x". If you are stuck on an item, you're expected to ask questions and give your best effort.

**Getting help on this assignment:** *You may work with others on this assignment, but you may not copy each others' answers.* Evidence of copying will be treated as academic dishonesty. You may also ask questions on

the #dailyprep channel on CampusWire, but you may not ask simply to be given the answers; giving and receiving answers on CampusWire will be treated as academic dishonesty.