



CSE 15: Discrete Mathematics

Homework 8

Fall 2020

Preliminary Notes

- **This homework must be solved individually.** You can discuss your ideas with others, but when you prepare your solution you must work individually. Your submission must be yours and yours only. No exceptions, and be reminded that the CSE academic honesty policy discussed in class will be enforced.
- Your solution must be exclusively submitted via CatCourses. Pay attention to the posted deadline because **the system automatically stops accepting submissions when the deadline passes. Late submissions will receive a 0.** You only need to submit the PDF and you have to use the template file provided in CatCourses. Please note that the system does not allow to submit any other file format. Do not submit the \LaTeX source of your solution.
- By now you should have become somewhat familiar with \LaTeX . You still will not be penalized for poor typesetting, but it is in your own interest to prepare your submission in a way that is easy to understand, so try using the appropriate \LaTeX symbols. If you do not know how to type a certain math symbol, search on the Internet and you will quickly find the answer.¹ **If in your \LaTeX submission you embed screenshots or scans of your handwritten solution those will not be graded.** You are encouraged to collaborate with other students to determine how to best format your submission or improve your \LaTeX skills.
- Start early.

1 The Division Algorithm

Using the result known as *division algorithm* presented in class, write the results of the following operations (carefully read the statement given in class to avoid making mistakes.)

a) $21 \text{ div } 4$

b) $13 \text{ mod } 5$

c) $-12 \text{ div } 5$

¹see <https://www.caam.rice.edu/~heinken/latex/symbols.pdf> for example.

2 Modular Arithmetic

Complete the following operations modulo m where $m = 13$.

a) $4 +_m 11$

b) $4 \cdot_m 11$

c) $23 +_m 54$

d) $7 \cdot_m (11 +_m 6)$

3 Trial Division for Prime Numbers

In class we have proven a theorem stating that if n is a composite integer, then it has a divisor less than or equal to \sqrt{n} . This theorem leads to a simple (but inefficient) algorithm to determine if an integer is prime or not, called the *trial division* method. Use the trial division method to show that 683 is a prime number.

Note: since you are already told that 683 is a prime number, just explain how you would use the trial division method to prove 683 is prime. You do not have to carry out all the operations because we already know the result.

4 Shift Cipher

Consider the case where plaintext messages are only composed of upper case letters of the English alphabet, plus spaces. Therefore there are 27 different symbols to represent (26 letters and the space). Consider an encoding where A is 0, B is 1, \dots , Z is 25, and the space is 26. Using the key $k = 7$ give the encoding of the following message using the shift cipher:

STUDY FOR THE FINAL