

CSE 015: Discrete Mathematics
Fall 2020
Homework #08
Solution

Tony Doan
Lab CSE-015-11L

December 12, 2020

1. Question 1: The Division Algorithm

- (a) $21 \text{ div } 4$
 $\frac{21}{4} = 5 \text{ remainder } 1$
 $= 5$
- (b) $13 \text{ mod } 5$
 $\frac{13}{5} = 2 \text{ remainder } 3$
 $= 3$
- (c) $-12 \text{ div } 5$
 $\frac{-12}{5} = -2 \text{ remainder } 2$
 $= -2$

2. Question 2: Modular Arithmetic

$m = 13$

- (a) $4 +_m 11$
 $(4 + 11) \text{ mod } 13$
 $15 \text{ mod } 13$
 $= 2$
- (b) $4 \cdot_m 11$
 $(4 \cdot 11) \text{ mod } 13$
 $44 \text{ mod } 13$
 $= 5$
- (c) $23 +_m 54$
 $(23 + 54) \text{ mod } 13$
 $77 \text{ mod } 13$

$$= 12$$

$$\begin{aligned} \text{(d)} \quad & 7 \cdot_m (11 +_m 6) \\ & 7 \cdot_m ((11 + 6) \bmod 13) \\ & 7 \cdot_m ((17) \bmod 13) \\ & 7 \cdot_m 4 \\ & (7 \cdot 4) \bmod 13 \\ & 28 \bmod 13 \\ & = 2 \end{aligned}$$

3. Question 3: Trial Division for Prime Numbers

The trial division algorithm takes in a number and divides it with a number greater than 1 and checks if the result has a remainder of 0. If the result has a remainder of 0, the program stores that number and takes the result and repeats the first step and divides the result with a number greater than 1 until it finds a result with a remainder of 0. This keeps on repeating until the program returns the result to be 1. All the numbers stored are the factors and can be used to determine if the given number is a composite or prime number.

We are given $n = 683$

- First we divide 683 by a number greater than 1, so 2:

$$683/2 = 341 \text{ remainder } 1$$

- Since the remainder is not 0, we continue and increment the divisor by 1:

$$683/3 = 227 \text{ remainder } 2$$

- We continue this process until the result is equal to 1 or the remainder is 0"

...

$$683/683 = 1 \text{ remainder } 0$$

- This has a remainder of 0 so it is stored into a list and the algorithm is over since the divisor is equal to the dividend.

Since 1 was the only number stored, the number 683 is a prime number.

4. Question 4: Shift Cipher

Given:

message = STUDY FOR THE FINAL

{A = 0, B = 1, ... , Z = 25, space = 26}

k = 7

Shift alphabet over by 7 to the right, so $\{A = 7, B = 8, \dots, Z = 5, \text{space} = 6\}$

Answer: $\{25, 26, 0, 10, 4, 6, 12, 21, 24, 6, 26, 14, 11, 6, 12, 15, 20, 7, 18\}$, 25260104612212462614116121520718