A5: NUMBER THEORY

**Do not worry about your difficulties in mathematics. I assure you that mine are greater.
—Albert Einstein (1879-1955)**

Course: CS 5002
Fall 2018
Due: 14 Oct 2018, Midnight

OBJECTIVES

After you complete this assignment, you will be comfortable with:

- Divisibility and modular arithmetic
- Primes, greatest common divisors (gcd) and largest common multipliers (lcm)
- Congruences and methods to solve them
- Some (cool) applications of congruences

RELEVANT READING

Rosen:

- 4.1: Divisibility and Modular Arithmetic
- 4.2: Integer Representations and Algorithms,
- 4.3: Primes and Greatest Common Divisors
- 4.4: Solving Congruences

NEXT WEEK'S READING

- Chapter 9: Relations

EXERCISES

Problem 1: Divisibility

Please find a div m and $a \bmod m$ when:

(a) $a = 123, m = 11$

(a) ______________________________

(b) $a = 55, m = 17$

(b) ______________________________

(c) $a = 1235, m = 35$

(c) ______________________________

(d) $a = 2357, m = 49$

(d) ______________________________

Problem 2: Divisibility and modular arithmetic

Please evaluate these quantities (please show your work/reasoning):

(a) $17 \bmod 9$

(a) ______________________________

(b) $-73 \bmod 5$

(b) ______________________________

(c) $-155 \bmod 12$

(c) ______________________________

(d) $300 \bmod 17$

(d) ______________________________

Problem 3: Modular arithmetic

What time does a 12-hour clock read (please show your work):

(a) 70 hours after it reads 9:00?

(a) ______________________________

(b) 45 hours after it reads 2:00?

(b) ______________________________

(c) 120 hours after it reads 7:00?

(c) ______________________________

Problem 4: Modular arithmetic

Determine whether each of these integer is congruent to 5 modulo 11 (please show your work):

(a) 38

(a) ______________________________

(b) 47

(b) ______________________________

(c) -65

(c) ______________________________

(d) -82

(d) ______________________________

Problem 5: Prime numbers

Determine whether or not the given integers are primes. Please show your work/reasoning:

(a) 13

(a) ______________________________

(b) 63

(b) ____________________

(c) 103

(c) ____________________

(d) 256

(d) ____________________

Problem 6: Prime and coprime numbers

Find all positive integers smaller than 35 that are relatively prime (coprime) to 35. Please show your work/reasoning.

Problem 7: Unique prime factorization

Find the unique prime factorization for each of the following integers. Please show your work.

(a) 99

(a) ____________________

(b) 432

(b) ____________________

(c) 10609

(c) ____________________

Problem 8: Euler ϕ function

Find the value of the Euler ϕ function for the following integers, n. Please show your work.

(a) $n = 15$

(a) ____________________

(b) $n = 17$

Problem 9: Euclidean algorithm

Use the Euclidean algorithm to find:

(a) (2 points) $\gcd(8, 25)$

(b) (3 points) $\gcd(78, 64)$

(c) (3 points) $\gcd(252, 300)$

Problem 10: Extended Euclidean algorithm

Use the extended Euclidean algorithm to express $\gcd(23, 68)$ as a linear combination of 23 and 68.

PROBLEMS

Problem 11: Divisibility

Show that an integer is divisible by 9 if and only if the sum of its decimal digits is divisible by 9.

Problem 12: Congruences

Find counterexamples for these statements about congruences:

(a) (4 points) If $ac \equiv bc \pmod{m}$, where a, b, c and m are integers with $m \geq 2$, then $a \equiv b \pmod{m}$.

(b) (4 points) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, where a, b, c, d and m are integers with c, d being positive, and $m \geq 2$, then $a^c \equiv b^d \pmod{m}$.

Problem 13: Modular arithmetic and congruences

Prove that $a \pmod{m} = b \pmod{m}$ if and only if $a \equiv b \pmod{m}$.

Problem 14: Modular arithmetic

Suppose that $a, m > 0$ and $a \not\equiv 0$ (mod m). Prove that

$$(-a) \bmod m = m - (a \bmod m).$$

Problem 15: Prime numbers and Euler ϕ-function

Show that some integer n is prime if and only if its **Euler ϕ-funtion** $\phi(n) = n - 1$.

Problem 16: Modular inverses

For each of the following pairs of integers (a, b), first determine whether or not $a^{-1} \bmod b$ exists. Then find $a^{-1} \bmod b$ if it exists. Show all work.

(a) $a = 5, b = 25$

(b) $a = 12, b = 29$

(c) $a = 24, b = 35$

(d) $a = 87, b = 102$

Problem 17: Fermat's Little Theorem

Chapter 4.4 of your textbook introduces an interesting and very valuable theorem, **the Fermat's little theorem**. Using that theorem, and the fact that numbers 103, 151, 167, 193 and 521 is a prime numbers, compute

(a) $7^{512} \pmod{103}$

(b) $3^{453} \pmod{151}$

(c) $2^{168} \pmod{167}$

(d) $15^{386} \pmod{193}$

(e) $5^{2082} \pmod{521}$

PROGRAMMING PROBLEMS

Problem 18: Pseudorandom number generator

The **power generator** is a method for generating pseudorandom numbers. To use the power generator, parameters p, d, and x_0 are specified, such that p is a prime numbers, d is a positive integer such that p does not divide d, and x_0 is a specified seed. The pseudorandom numbers $x_1, x_2, \dots$ are generated using the following recursive definition:

$$x_{n+1} = x_n^d \pmod{p} \tag{1}$$

Write a Python function that takes in four parameters parameters:

- Prime number p
- Positive integer d
- Seed x_0
- The length of the sequence of pseudorandom numbers to be generated, n

Your function should compute, and print on the screen the sequence of n pseudorandom numbers, generated using power generator described above.

For full credit, provide your code, and ensure that it is readable. We should be convinced that it works by reading it, without necessarily running it.

Problem 19: Valid USPS Money Orders

The United States Postal Service (USPS) sells money orders identified by an 11-digit number $x_1x_2x_3\dots x_{11}$. The first ten digits identify the money order, and the last one x_{11} is a check digit that satisfies:

$$x_{11} = x_1 + x_2 + \dots x_{10} \pmod{9}$$

Write a Python function that takes one input argument, a 5-digit number, and similar to the validity check for the USPS mony order, check whether or not the given number is valid by checking that the last digit satisfies equation:

$$x_5 = x_1 + x_2 + x_3 + x_4 \pmod 5$$

Your function should return true if the given digit is valid, and false otherwise. For full credit, provide your code, and ensure that it is readable. We should be convinced that it works by reading it, without necessarily running it.

Problem 20: Shift Cipher

The **Shift cipher** is one of the oldest known cryptosystems, often attributed to Julius Caesar. The idea used in this cryptosystem is to replace each letter in an alphabet by another letter at a distance K from it.

Formally, let's associate each letter $A, B, ..., Z$ with an integer $0, \ldots, 25$. If we allow the key K to be any integer with $0 \leq K \leq 25$, the *shift cipher* can be defined as:

$$\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}.$$
$$\text{For } 0 \leq K \leq 25,$$

$$\begin{aligned} y &= e_K(x) = (x + K) \bmod 26, \\ x &= d_K(y) = (y - K) \bmod 26. \end{aligned}$$

The following ciphertext was encrypted by a *shift cipher*:

```
ycvejqwvhqtdtwvwu
```

Please decrypt it.

Question	Points	Score
Divisibility	4	
Divisibility and modular arithmetic	4	
Modular arithmetic	3	
Modular arithmetic	4	
Prime numbers	2	
Prime and coprime numbers	4	
Unique prime factorization	6	
Euler ϕ function	2	
Euclidean algorithm	8	
Extended Euclidean algorithm	5	
Divisibility	6	
Congruences	8	
Modular arithmetic and congruences	5	
Modular arithmetic	4	
Prime numbers and Euler ϕ-function	4	
Modular inverses	6	
Fermat's Little Theorem	5	
Pseudorandom number generator	6	
Valid USPS Money Orders	7	
Shift Cipher	7	
Total:	100	

SUBMISSION DETAILS

Things to submit:

- Submit the following on Blackboard for Assignment 5:
  - The written parts of this assignment as a .pdf named "CS5002_[lastname]_A5.pdf". For example, my file would be named "CS5002_Bonaci_A5.pdf". (There should be no brackets around your name).
  - Make sure your name is in the document as well (e.g., written on the top of the first page).