HW7: INTRODUCTION TO NUMBER THEORY

"Some numbers, even large ones, have no factors— except themselves, of course, and 1. These are called prime numbers, because everything they are starts with themselves. They are original, gnarled, unpredictable, the freaks of the number world." — Richard Friedberg

Course: CS 5002
Fall 2021
Due: Saturday, November 13, 2021

PROBLEMS

Problem 1: Divisibility and modular arithmetic

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

(a) (2 points) $17 \bmod 9$

(a)

$$17 \; mod \; 9 = 17 - \left\lfloor \frac{17}{9} \right\rfloor \cdot 9 = 17 - 9 = 8$$

(b) (2 points) $-73 \bmod 5$

(b)

$$-73 \; mod \; 5 = -73 - \left\lfloor \frac{-73}{5} \right\rfloor \cdot 5 = -73 - (-15 \cdot 5) = 2$$

(c) (2 points) $-155 \bmod 12$

(c)

$$-155 \; mod \; 12 = -155 - \left\lfloor \frac{-155}{12} \right\rfloor \cdot 12 = -155 - (-13 \cdot 12) = 1$$

(d) (2 points) $300 \bmod 17$

(d)

$$300 \; mod \; 17 = 300 - \left\lfloor \frac{300}{17} \right\rfloor \cdot 17 = 300 - (17 \cdot 17) = 11$$

Points: _____ out of 8

Problem 2: Modular arithmetic

Determine whether each of these integer is congruent to 5 modulo 11. Please show your work.

(a) (2 points) 38

(a)

$$5\ mod\ 11 = 5$$

$$38\ mod\ 11 = 38 - \left\lfloor \frac{38}{11} \right\rfloor \cdot 11 = 38 - 33 = 5$$

Therefore, 38 and 5 mod 11 are congruent.

(b) (2 points) 47

(b)

$$5\ mod\ 11 = 5$$

$$47\ mod\ 11 = 47 - \left\lfloor \frac{47}{11} \right\rfloor \cdot 11 = 47 - 44 = 3$$

Therefore, 47 and 5 mod 11 are not congruent.

(c) (2 points) -65

(c)

$$5\ mod\ 11 = 5$$

$$-65\ mod\ 11 = -65 - \left\lceil \frac{-65}{11} \right\rceil \cdot 11 = -65 + 66 = 1$$

Therefore, -65 and 5 mod 11 are not congruent.

(d) (2 points) -82

(d)

$$5\ mod\ 11 = 5$$

$$-82\ mod\ 11 = -82 - \left\lceil \frac{-82}{11} \right\rceil \cdot 11 = -82 + 88 = 6$$

Therefore, -82 and 5 mod 11 are not congruent.

Problem 3: Unique prime factorization

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

(a) (2 points) 99

(a)

$$99 = 3 * 33 = 3 * 3 * 11 = 3^2 * 11$$

(b) (2 points) 432

(b)

$$432 = 2 * 216 = 2 * 2 * 108 = 2 * 2 * 2 * 54 = 2 * 2 * 2 * 2 * 27 = 2 * 2 * 2 * 2 * 3 * 9$$
$$= 2 * 2 * 2 * 2 * 3 * 3 * 3 = 2^4 * 3^3$$

(c) (2 points) 10609

(c)

$$10609 = 103 * 103 = 103^2$$

Problem 4: Euler ϕ function

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

(a) (2 points) $n = 15$

(a)

$$\varphi(15) = \varphi(3 \cdot 5) = 15 \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) = 8$$

(b) (2 points) $n = 17$

(b)

$$\varphi(17) = \varphi(17) = 17 \cdot \left(1 - \frac{1}{17}\right) = 16$$

Problem 5: Inverse modulo

Find an inverse of a modulo m for each of these pairs of relatively prime integers using the extended Euclidean algorithm.

(a) (5 points) a = 2, m = 17

.
(a)
gcd(17, 2)
y = 17, x = 2
r = y mod x = 17 - (17 div 2) * 2 = 1
y = 2, x = 1
r = y mod x = 2 - (2 div 1) * 1 = 0
Therefore, gcd(17, 2) = 1 = 1 * 17 - 8 * 2
The inverse of 2 mod 17 is (c mod 17), where c is the coefficient of 2:
-8 mod 17 = 9

(b) (5 points) a = 34, m = 89

(b)
gcd (89, 34)
y = 89, x = 34
r = y mod x = 89 - (89 div 34) * 34 = 21
y = 34, x = 21
r = y mod x = 34 - (34 div 21) * 21 = 13
y = 21, x = 13
r = y mod x = 21 - (21 div 13) * 13 = 8
y = 13, x = 8
r = y mod x = 13 - (13 div 8) * 8 = 5
y = 8, x = 5
r = y mod x = 8 - (8 div 5) * 5 = 3
y = 5, x = 3
r = y mod x = 5 - (5 div 3) * 3 = 2
y = 3, x = 2
r = y mod x = 3 - (3 div 2) * 2 = 1
y = 2, x = 1
r = y mod x = 2 - (2 div 1) * 1 = 0
Therefore, gcd(89, 34) = 1
= 3 - 2
= 3 - (5 - 3)
= 2 * 3 - 1 * 5
= 2 * (8 - 5) - 1 * 5
= 2 * 8 - 3 * 5
= 2 * 8 - 3 * (13 - 8)
= 5 * 8 - 3 * 13
= 5 * (21 - 13) - 3 * 13
= 5 * 21 - 8 * 13
= 5 * 21 - 8 * (34 - 21)
= 13 * 21 - 8 * 34
= 13 * (89 - 2 * 34) - 8 * 34
= 13 * 89 - 34 * 34
The inverse of 34 mod 89 is (c mod 89), where c is the coefficient of 34:
-34 mod 89 = 55

Problem 6: Linear congruanges

Please consider the following linear congruence, and solve for x, using the steps outlined below.

$$57x + 13 = 5 \pmod{17}$$

(a) (4 points) Use the Euclidean algorithm to find the correct GCD of numbers 57 and 17.

(a)
57 mod 17
y = 57, x = 17
r = y mod x = 57 - (57 div 17) * 17 = 6
y = 17, x = 6
r = y mod x = 17 - (17 div 6) * 6 = 5
y = 6, x = 5
r = y mod x = 6 - (6 div 5) * 5 = 1
y = 6, x = 1
Therefore, the gcd of 57 and 17 is 1.

(b) (5 points) Use the Extended Euclidean algorithm to find the Bezout coefficients.

(b)
gcd (57, 17) = 1
= 6 - 5
= 6 - (17 - 2 * 6)
= 3 * 6 - 1 * 17
= 3 * (57 - 3 * 17) - 1 * 17
= 3 * 57 - 10 * 17

(c) (5 points) Solve for x.

(c)
57x + 13 = 5 mod 17
57x = -8 mod 17
The multiplicate inverse of 57 mod 17 is 3.
(3 * 57) x = 3 * 9 mod 17
x = 27 mod 17 = 10 + 17n, where n can be integer.

Problem 7: Divisibility

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

Proof:

If the sum of the digits of n is divisible by 9, then n is divisible by 9.

If n is divisible by d iff there exists some integer k such that n = dk

d | n

Decimal representation of n:

$$n = d_k 10^k + d_{k-1}10^{k-1} + d_{k-2}10^{k-2} + \cdots + d_1 10 + d_0$$

$$n = d_k(10^k - 1 + 1) + d_{k-1}(10^{k-1} - 1 + 1) + d_{k-2}(10^{k-2} - 1 + 1) + \cdots + d_1(10 - 1 + 1) + d_0$$

$$n = d_k(10^k - 1) + d_{k-1}(10^{k-1} - 1) + d_{k-2}(10^{k-2} - 1) + \cdots + d_1(10 - 1) + (d_k + \cdots + d_0)$$

For every 10^m - 1, it will be a number consisting only 9's, which means that 10^m - 1is divisible by 9, such that 10^m - 1 = $9c_m$. Therefore:

$$n = d_k c_k 9 + d_{k-1}c_{k-1}9 + \cdots + d_1 c_1 9 + (d_k + \cdots + d_0)$$

Since, $d_k + \cdots + d_0$ is the sum of all the decimal digits of number n, only if the sum of all digits is divisible by 9, that n is divisible by 9, and it is the same other way. ■

Problem 8: Congruences

Find counterexamples for these statements about congruences:

(a) (3 points) If $ac \equiv bc \pmod{m}$, where a, b, c and m are integers with $m \geq 2$, then $a \equiv b \pmod{m}$.

(a)

If c = 0, then ac = 0, bc = 0, then ac mod m = bc mod m = 0, therefore, although a does not equal to b, ac = bc (mod m) = 0.

(b) (3 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 $a^c \equiv b^d \pmod{m}$.

(b)
If a = 3, b = 3, c = 1, d = 6, m = 5, then, c = d mod m, a = b mod m,
$a^c = 3 \bmod 5 = 3$
$b^d = 3^6 = 729 \bmod 5 = 4$,
Therefore, a^c and b^d are not equal mod 5.

Problem 9: Prime numbers and Euler ϕ-function

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

Proof:
If integer n is prime, it only has itself as its factor:

$$\varphi(n) = n \cdot \left(1 - \frac{1}{n}\right) = n \cdot \left(\frac{n-1}{n}\right) = n - 1$$

If $\varphi(n) = n - 1$, then all numbers less than n are coprime to integer n, which means n is prime.
Therefore, n is prime iff its Euler function $\varphi(n) = n - 1$.■

Problem 10: ISBN Numbers

The check digit a_{13} for an ISBN-13 with initial digits $a_1 a_2 \ldots a_{12}$ is determined by the congruence $(a1 + a3 + \cdots + a13) + 3(a2 + a4 + \cdots + a12) \equiv 0 (\mathrm{mod} 10)$.

Determine whether each of these 13-digit numbers is a valid ISBN-13.

(a) (5 points) 978-0-073-20679-1

(a)

$(a1 + a3 + \cdots + a13) + 3(a2 + a4 + \cdots + a12)$

$= (9 + 8 + 0 + 3 + 0 + 7 + 1) + 3(7 + 0 + 7 + 2 + 6 + 9)$

$= 28 + 3(31) = 28 + 93 = 121$

121 mod 10 = 1, which is not equal to 0, so this is not a valid ISBN number.

(b) (5 points) 978-3-16-148410-0

(b)

$(a1 + a3 + \cdots + a13) + 3(a2 + a4 + \cdots + a12)$

$= (9 + 8 + 1 + 1 + 8 + 1 + 0) + 3(7 + 3 + 6 + 4 + 4 + 0)$

$= 28 + 3(24) = 28 + 72 = 100$

100 mod 10 = 0, which is equal to 0, so this is a valid ISBN number.

Problem 11: Cryptography

In this question, we're going to explore some common ways to encrypt and decrypt messages. Get your calculators ready! For the next few questions, please use this table:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

(a) First up is the Caesar cipher. Julius Caesar sent messages to his friends by converting a letter to a number, adding three to the number, taking that number $\mod 26$, and converting it back into a letter. Decrypt these messages that were encrypted using the Caesar cipher.

i. (3 points) EOXH MHDQV

(a)(i)
The initial letter value cannot be greater than 25.
x + 3 mod 26
E = 4: x + 3 = 4 mod 26, so x = 1, initial letter B
O = 14: x + 3 = 14 mod 26, so x = 11, initial letter L
X = 23: x + 3 = 23 mod 26, so x = 20, initial letter U
H = 7: x + 3 = 7 mod 26, so x = 4, initial letter E
M = 12, so x = 9, initial letter J
H = 7, so x = 4, initial letter E
D = 3, so x = 0, initial letter A
Q = 16, so x = 13, initial letter N
V = 21, so x = 18, initial letter S

The initial message is BLUE JEANS.

ii. (3 points) WHVW WRGDB

(a)(ii)
W = 22, initial 22 - 3 = 19, T
H = 7, initial 7 - 3 = 4, E
V = 21, initial S
W = 22, initial 22 - 3 = 19, T

W = T
R = 17, initial 17 - 3 = 14, O
G = 6, initial 6 - 3 = 3, D
D = 3, initial 3 - 3 = 0, A
B = 1, initial 1 - 3 = -2, Y

The initial message is TEST TODAY.

(b) (5 points) A slightly more advanced version of the Caesar cipher is the shift cipher, where instead of adding 3 to the number, you add k. That gives us an encryption function of $f(p) = p + k \mod 26$ (for Caesar, $k = 3$). Encrypt the message WATCH YOUR STEP by translating the letters into numbers, applying the encryption function below, and then translating the numbers back into letters.

$f(p) = (p + 14) \mod 26$

(b)
WATCH YOUR STEP
22, 0, 19, 2, 7, 24, 14, 20, 17, 18, 19, 4, 15.
Applying the translation function f(p) = (p + 14) mod 26, we get:
10, 14, 7, 16, 21, 12, 2, 8, 5, 6, 7, 18, 3
Translating the above number to letters:
KOHQV MCIF GHSD

(c) (9 points) An even more advanced version is the *affine cipher*, where the encryption function takes the form $f(p) = (ap + b) \mod 26$, where a and b are integers chosen such that $f(p)$ is a bijection. In the Caesar cipher, $a = 1$ and $b = 3$. In the shift cipher, $a = 1$ and $b = k$.

The encrypted version of a message is LJMKG MGMXF QEXMW. If it was encrypted using the affine cipher $f(p) = (7p + 10) \mod 26$, what was the original message? (Please note: the spacing in the encrypted message is to make it easy to read: spaces do not denote the original word boundaries).

Take a good stab at approaching this problem. If you need a hint at some point, ask.

(c)
f(p) = (7p + 10) mod 26
LJMKG MGMXF QEXMW
11, 9, 12, 10, 6, 12, 6, 12, 23, 5, 16, 4, 23, 12, 22
y = 26, x = 7
r = 26 - 3 * 7 = 5
y = 7, x = 5
r = 7 - 5 = 2
y = 5, x = 2
r = 5 - 2 * 2 = 1
y = 2, x = 1
gcd (26, 7) = 1
1 = 2 - 1
1 = 2 - (5 - 2 * 2) = 3 * 2 - 1 * 5
1 = 3 * (7 - 5) - 1 * 5
1 = 3 * 7 - 4 * 5
1 = 3 * 7 - 4 * (26 - 3 * 7)
1 = 15 * 7 - 4 * 26
The multiplicative inverse of 7 mod 26 is 15.
7p + 10 mod 26
L: 7p = 1 mod 26, (7 * 15) p = (1 * 15) mod 26 = 15, P
J: 7p = -1 mod 26, (7 * 15) p = (-1 * 15) mod 26 = 11, L
M: 7p = 2 mod 26, (7 * 15) p = (2 * 15) mod 26 = 4, E
K: 7p = 0 mod 26, (7 * 15) p = 0 mod 26 = 0, A
G: 7p = -4 mod 26, (7 * 15) p = (-4 * 15) mod 26 = 18, S
M: E
G: S
M: E
X: 7p = 13 mod 26, (7 * 15) p = (13 * 15) mod 26 = 13, N
F: 7p = -5 mod 26, (7 * 15) p = (-5 * 15) mod 26 = 3, D
Q: 7p = 6 mod 26, (7 * 15) p = (6 * 15) mod 26 = 12, M
E: 7p = -6 mod 26, (7 * 15) p = (-6 * 15) mod 26 = 14, O
X: N
M: E
W: 7p = 12 mod 26, (7 * 15) p = (12 * 15) mod 26 = 24, Y
The initial message is PLEASE SEND MONEY.

Question	Points	Score
Divisibility and modular arithmetic	8	
Modular arithmetic	8	
Unique prime factorization	6	
Euler ϕ function	4	
Inverse modulo	10	
Linear congruanges	14	
Divisibility	10	
Congruences	6	
Prime numbers and Euler ϕ-function	4	
ISBN Numbers	10	
Cryptography	20	
Total:	100	

SUBMISSION DETAILS

Things to submit:

- Please submit this assignment as a .pdf named "CS5002_[lastname]_HW7.pdf" through Canvas by 11:59pm PST on Saturday, November 13, 2021.
- Please make sure your name is in the document as well (e.g., written on the top of the first page).