Exercises: Modular Arithmetic 1 - Solutions

Exercise 1

This exercise practices the basic skills you need to solve the subsequent exercises.

1.1 Divisors

Find all the divisors of the following numbers:

a. $1, 2, 5, 10$
b. 1,11
c. $1, 2, 3, 4, 6, 12$
d. 1,13
e. $1, 3, 9, 11, 33, 99$
f. $1, 2, 4, 5, 10, 20, 25, 50, 100$

Determine whether each of the following are true:

a. True
b. False
c. False
d. True

1.2 Remainders

Find the remainders below:

a. 5
b. 0
c. 2
d. 0
e. 20
f. 8

1.3 Primes

Which of the following statements about primes are true?

a. False
b. True
c. False
d. False

Which of the following numbers are primes?

a. Not prime
b. Prime
c. Not prime
d. Prime
e. Prime
f. Not prime

Exercise 2

Find the prime factorization of

a. $2^3 \cdot 3 \cdot 5$
b. $5^3 \cdot 3$
c. 47
d. $3 \cdot 5 \cdot 11 \cdot 13$

Exercise 3

In exercise 1.1 you found all the divisors of a list of numbers. Use these results to find the greatest common divisors below:

a. 2
b. 1
c. 1
d. 1
e. 10
f. 1

Exercise 4

Use Euclid's algorithm to find the greatest common divisor in each of the following pairs of numbers:

a. 3
b. 2
c. 1

Exercise 5

Two numbers, a and b, are called relatively prime if $\gcd(a, b) = 1$. Answer the questions below.

a. Yes
b. Yes
c. No
d. No
e. No
f. Yes

Exercise 6

If n is some positive integer, we can calculate how many of the numbers between 1 and n that are relatively prime to n as $\varphi(n)$ - this function is called Euler's phi-function. Use Euler's phi-function to answer the following questions:

a. 4
b. 16
c. 8
d. 6
e. 20
f. 4

Exercise 7

Two numbers are said to be "congruent to each other modulo n'' if they have the same remainder after division by n. For example, 1 is congruent to 11 modulo 5 , because both have the same remainder after division by 5: $\text{rem}(1, 5) = \text{rem}(11, 5)$. Which of the following numbers are congruent to each other modulo 4 ?

a. Yes
b. No
c. Yes
d. Yes
e. Yes
f. No

Exercise 8

If a is congruent to b modulo n, we can write this as $a \equiv b(\text{mod} n)$. For example, the statement that 1 is congruent to 11 modulo 5 can be written as $1 \equiv 11 \pmod 5$. Use this notation to write each of the statements from exercise 9 to which the answers was yes.

$1 \equiv 5(\text{mod}4)$,
$0 \equiv 4(\text{mod}4)$,
$0 \equiv 8(\text{mod}4)$,
$3 \equiv 7(\text{mod}4)$

Exercise 9

Just as regular arithmetic revolves around the equality symbol, =, (e.g. solving equations like $5x\ 3 = 7$), modular arithmetic revolves around the congruence symbol, $\equiv (\text{mod} n)$. So in modular arithmetic, we solve congruences like $5x - 3 \equiv 7 \pmod 4$. Solve each of the congruences below (you are allowed to add or subtract on both sides just like in regular arithmetic):

a. $x \equiv 1(\text{mod}4)$
b. $x \equiv -1(\text{mod}4)$
c. $x \equiv 13(\text{mod}4)$
d. $x \equiv 2(\text{mod}7)$
e. $x \equiv -1(\text{mod}5)$

Exercise 10

In each of the exercises in exercise 11 , find the smallest positive value for x which fulfills the congruence.

a. $x \equiv 1(\text{mod}4)$
b. $x \equiv 3(\text{mod}4)$
c. $x \equiv 1(\text{mod}4)$
d. $x \equiv 2(\text{mod}7)$
e. $x \equiv 4(\text{mod}5)$