

MAT 112

Integers and Modern Applications for the Uninitiated

<https://go.uncg.edu/mat112>

Workbook^{1 2}

Chaichana Prasertsrithong and Sebastian Pauli

Department of Mathematics and Statistics
University of North Carolina Greensboro

August 12, 2026

¹The problems in this workbook were exported from ©WeBWorK, Mathematical Association of America (<http://webwork.maa.org>).

²This work is licensed under the Creative Commons Attribution Non-Commercial Share-Alike 4.0 International License (<http://creativecommons.org/licenses/by-nc-sa/4.0>).

Contents

1	Foundations	5
1.1	Integers	6
1.2	Statements	13
1.3	Variables	17
1.4	Exponentiation	25
2	Algorithms	32
2.2	return	33
2.3	if-then	37
2.4	let	41
2.5	repeat-until	45
2.6	Exponentiation Algorithm	50
3	Division	55
3.1	Quotients and Remainders	56
3.2	Division Algorithm	59
3.3	Long Division	71
3.4	Operation mod	75
3.5	Clock Arithmetic	85
3.6	ISBN	88
4	Greatest Common Divisors	93
4.1	Divisibility	94
4.2	Greatest-Common-Divisors	98
4.3	Euclidean-Algorithm	103
4.4	Bezouts-Identity	108
5	Sets	113
5.1	Sets	114
5.2	Roster Form	117
5.3	Membership and Equality	120
5.4	Special Sets	126
5.5	Set Builder Notation	131

6	More on Sets	135
6.1	Subsets	136
6.2	Cartesian Products	143
6.3	Applications of Cartesian Products	147
7	Functions	150
7.1	Definition of Function	151
7.2	Equality of Functions	162
7.3	Composite Functions	170
7.4	Identity Functions	175
7.5	Inverse Functions	183
8	Codes	193
8.1	Character Encoding	194
8.2	Symmetric Key Cryptography	197
8.3	Caesar Ciphers	200
8.4	Other Substitution Ciphers	205
8.5	Frequency Analysis	212
9	Cardinality	222
9.1	Definition of Cardinality	223
9.2	Infinite Sets	227
9.3	Cardinality of Cartesian Products	231
9.4	Number of Subsets	234
10	Primes	237
10.1	Definition of a Prime	238
10.2	Sieve of Eratosthenes	241
10.3	Prime Factorization	245
10.4	Infinitude of Primes	255
10.5	Twin Prime Conjecture	258
11	Other Bases	263
11.1	Decimal Representation	264
11.2	Binary Representation	266
11.3	From Decimal to Binary	273
11.4	Base b Numbers	277
11.5	From Decimal to Base b	285
12	Applications of other Bases	291
12.1	Images	292
12.2	Colors	300
12.3	Text	308

13 Binary Operations	312
13.1 Definition of Binary Operation	313
13.2 Associativity	318
13.3 Identity	320
13.4 Inverses	327
13.5 Commutativity	335
14 Groups	340
14.1 Definition of Group	341
14.2 Examples of Groups	344
14.3 Modular Arithmetic	354
14.4 Additive Groups	359
14.5 Multiplicative Groups	364
15 Powers and Logarithms	371
15.1 Exponentiation	372
15.2 Repeated Squaring	380
15.3 Fast Exponentiation	387
15.4 Discrete Logarithm	396
16 Public Key Cryptography	403
16.1 Introduction Public Key	404
16.2 Diffie Hellman	407
16.3 ElGamal Crypto System	415

Chapter 1

Foundations

1. Integers
2. Statements
3. Variables
4. Exponentiation

1.1 Integers

Problem 1.1 (1) Fill in the blank.

The numbers $1, 2, 3, 4, \dots$ are the _____.

(Check all that apply)

- A. natural numbers
- B. odd numbers
- C. negative integers
- D. positive integers
- E. integers
- F. even numbers

Hint: More than one answer might be correct. Check all that apply.

Problem 1.1 (2) Fill in the blank.

The numbers $\dots, -4, -3, -2, -1$ are the _____.

(Check all that apply)

- A. positive integers
- B. even integers
- C. negative integers
- D. integers
- E. natural numbers
- F. odd integers

Hint: More than one answer might be correct. Check all that apply.

Problem 1.1 (3)

Complete this the operation table for subtraction. In each table cell enter the heading of the row minus the heading of the column heading.

—	-3	-2	-1	0	1	2
-1	2	1	0	—	—	—
0	3	—	—	—	—	-2
1	4	3	—	—	0	-1
2	—	4	3	—	—	0
3	—	—	—	—	—	—
4	—	—	—	4	—	—

Problem 1.1 (4)

Complete this the operation table for addition. In each table cell enter the heading of the row plus the heading of the column heading.

+	0	1	2	3	4	5	6
-2	—	—	—	1	—	—	—
-1	—	0	—	2	—	4	5
0	—	—	2	3	4	—	—
1	1	—	—	4	—	6	7
2	—	—	—	—	—	—	8
3	3	—	—	—	7	—	9
4	—	—	—	—	8	—	10

Problem 1.1 (5) (1 point)

Subtract the following integers:

$$4 - 6 = \underline{\hspace{2cm}}$$

$$10 - 2 = \underline{\hspace{2cm}}$$

$$2 - 17 = \underline{\hspace{2cm}}$$

Problem 1.1 (6) (1 point)

Multiply the following integers.

a. $(-9) \cdot (-1) = \underline{\hspace{2cm}}$

b. $(-5) \cdot 2 = \underline{\hspace{2cm}}$

c. $6 \cdot (-7) = \underline{\hspace{2cm}}$

d. $(-6) \cdot 0 = \underline{\hspace{2cm}}$

Problem 1.1 (7) (1 point)

Add the following:

$$-8 + (-2) = \underline{\hspace{2cm}}$$

$$-6 + (-5) = \underline{\hspace{2cm}}$$

$$-1 + (-8) = \underline{\hspace{2cm}}$$

Solutions

Problem 1.1 (1) *Correct Answers:*

- AD

Problem 1.1 (2) *Correct Answers:*

- C

Problem 1.1 (3) *Correct Answers:*

—	-3	-2	-1	0	1	2
-1	2	1	0	-1	-2	-3
0	3	2	1	0	-1	-2
1	4	3	2	1	0	-1
2	5	4	3	2	1	0
3	6	5	4	3	2	1
4	7	6	5	4	3	2

Problem 1.1 (4) *Correct Answers:*

+	0	1	2	3	4	5	6
-2	-2	-1	0	1	2	3	4
-1	-1	0	1	2	3	4	5
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	7
2	2	3	4	5	6	7	8
3	3	4	5	6	7	8	9
4	4	5	6	7	8	9	10

Problem 1.1 (5) *Correct Answers:*

Solution:

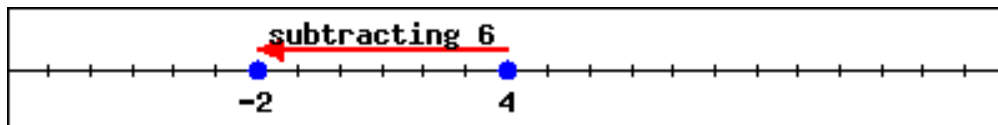
It helps to understand that the subtraction sign means that we are adding the opposite. For example, $3 - 2 = 3 + (-2)$. For many students, it's easier to change “minus a number” into “adding the opposite number”. This way of looking at subtraction will help us understand more complicated topics later, like subtracting a negative number.

METHOD 1

One way is to use a number line. Let's do this for $4 - 6$. First, we rewrite it as

$$4 + (-6)$$

Find 4 on a number line. Since we are adding a negative number, we move left, in the negative direction, by 6 units. We will reach -2 on the number line, which is the answer.



So $4 - 6 = -2$.

Similarly, $10 - 2 = 8$ and $2 - 17 = -15$.

METHOD 2

A second method asks you to think in context; for example when money is involved or the temperature changes. Let's do this for $4 - 6$. First, we rewrite it as

$$4 + (-6).$$

The first number is 4. Since it's positive, it's like you won 4 dollars at the casino this morning.

The second number is -6 . Since it's negative, it's like you lost 6 dollars in the casino later this afternoon.

Since you lost more money than you won, you ended up losing money overall, implying the answer is negative.

Since you won 4 dollars and then lost 6 dollars, it makes sense that you lost the difference of 6 and 4 dollars, which is 2 dollars. So the final answer is: $4 - 6 = -2$.

Correct Answers:

- -2
- 8
- -15

Problem 1.1 (6) *Correct Answers:*

Solution:

The rules for multiplying positive and negative numbers are:

- positive $\cdot$ positive = positive,
- positive $\cdot$ negative = negative,
- negative $\cdot$ positive = negative,
- negative $\cdot$ negative = positive.

The solutions are:

- a. $(-9) \cdot (-1) = 9$,
- b. $(-5) \cdot 2 = -10$,
- c. $6 \cdot (-7) = -42$,
- d. $(-6) \cdot 0 = 0$.

Correct Answers:

- 9
- -10
- -42
- 0

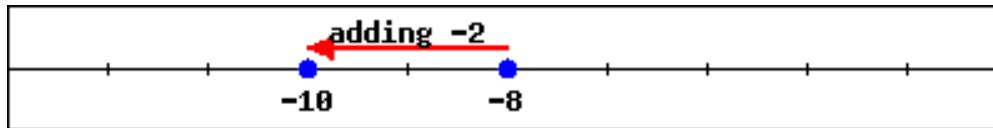
Problem 1.1 (7) Correct Answers:**Solution:**

Here are two different explanations of how two negative numbers can be added together.

METHOD 1

Use a number line. Let's find $-8 + (-2)$.

First, find -8 on the number line. Next, since we are adding a negative number, we move left, in the negative direction, by 2 units. We will reach -10 on the number line, which is the answer.



So, $-8 + (-2) = -10$.

Similarly, $-6 + (-5) = -11$, and $-1 + (-8) = -9$.

METHOD 2

A second method asks you to think in terms of money. Let's find $-8 + (-2)$.

The first number is -8 . Since it's negative, it's like you lost 8 dollars while gambling at the casino this morning.

The second number is -2 . Since it's negative, it's like you lost 2 dollars again while gambling in the casino this afternoon.

Since you lost twice, you ended up losing a lot, implying the answer is negative.

Since you lost 8 dollars and then lost 2 dollars, it makes sense that you lost a total of 10 dollars. So the final answer is: $-8 + (-2) = -10$.

Correct Answers:

- -10
- -11
- -9

1.2 Statements

Problem 1.2 (1) (1 point)

For each of the following choose the comparison symbol that yields a true statement:

-53 _____ 94

[select: ☐ = ☐ $\neq$ ☐ < ☐ > ☐ $\geq$ ☐ $\leq$]

85 _____ 85

[select: ☐ = ☐ $\neq$ ☐ < ☐ > ☐ $\geq$ ☐ $\leq$]

Problem 1.2 (2)

For each line select the comparison that yields a true statement:

119 _____ 54

[select: ☐ is less than ☐ is equal to ☐ is less than or equal to ☐ is greater than or equal to ☐ cannot be compared to]

93 _____ 119

[select: ☐ is less than ☐ is equal to ☐ is less than or equal to ☐ is greater than or equal to ☐ cannot be compared to]

Problem 1.2 (3)

For each line select the comparison that yields a true statement:

-40 _____ -500

[select: ☐ is less than ☐ is equal to ☐ is greater than ☐ cannot be compared to]

-109 _____ -293

[select: ☐ is less than ☐ is equal to ☐ is greater than ☐ cannot be compared to]

-293 _____ -17

[select: ☐ is less than or equal to ☐ is equal to ☐ is greater than or equal to ☐ cannot be compared to]

Problem 1.2 (4)

For each of the following decide whether it is a statement.
If it is a statement decide whether it is a true or false.

1. _____ $25 + 9 \neq 375$
2. _____ $15 \cdot (25 - 9)$
3. _____ $9 + 25$
4. _____ $(25 + 25) \cdot 15$

Problem 1.2 (5)

Determine which of the following are mathematical statements.
For the statements decide whether they are true or false.

1. _____ $26 < 26$
2. _____ $13 \geq 13$
3. _____ $13 - (-26)$
4. _____ $-26 > 26$

Problem 1.2 (6)

Determine which of the following are mathematical statements.
Recall that a statement is either true or false.

1. _____ $-29 - 28$
2. _____ $7 = 28$
3. _____ $28 \cdot (-29)$
4. _____ $7 \geq 7$

Problem 1.2 (7)

Enter a T or an F in each answer space below to indicate whether the corresponding statement is true or false.

You must get all of the answers correct to receive credit.

- ___1. $-4 < -7$
- ___2. $-9 < -9$
- ___3. $-4 > -7$

___4. $-8 \geq -8$

Notice that if one of your answers is wrong then, in this problem, WeBWorK will tell you which parts are wrong and which parts are right. This is the behavior for most problems, but for true/false or multiple choice questions WeBWorK will usually only tell you whether or not all the answers are correct. It won't tell you which ones are wrong. The idea is to encourage you think rather than to just try guessing.

In every case all of the answers must be correct before you get credit for the problem.

Solutions

Problem 1.2 (1) *Correct Answers:*

- $<$
 - $=$
-

Problem 1.2 (2) *Correct Answers:*

- is greater than or equal to
 - is less than
-

Problem 1.2 (3) *Correct Answers:*

- is greater than
 - is greater than
 - is less than or equal to
-

Problem 1.2 (4) *Correct Answers:*

- True Statement
 - Not a Statement
 - Not a Statement
 - Not a Statement
-

Problem 1.2 (5) *Correct Answers:*

- F
 - T
 - N
 - F
-

Problem 1.2 (6) *Correct Answers:*

- N
 - S
 - N
 - S
-

Problem 1.2 (7) *Correct Answers:*

- F
- F
- T
- T

1.3 Variables

Problem 1.3 (1) (1 point)

Let $a := 7$ and $n := 3$ and $j := 11$. Evaluate the following:

$$a \cdot n = ______$$

$$n \cdot a = ______$$

$$a - n = ______$$

$$n - a = ______$$

$$n + (a + j) = ______$$

$$(n + a) + j = ______$$

$$(a \cdot j) - (n \cdot j) = ______$$

$$(a - n) \cdot j = ______$$

$$(a \cdot n) - j = ______$$

$$n \cdot (a - j) = ______$$

Problem 1.3 (2) (1 point)

Let $f := 2$ and $q := 4$. Evaluate the following:

$$(-6) \cdot (f \cdot f) = ______$$

$$((f - q) \cdot (f - q)) + 8 = ______$$

$$(8 \cdot f) - (6 \cdot q) = ______$$

$$(q - 5) + (6 \cdot f) = ______$$

Problem 1.3 (3) (1 point)

Let $d := -4$.

Decide which of the following are statements, true statements, or false statements.

1. _____ $d = -4$
2. _____ $d < 3$
3. _____ $3 = d$
4. _____ $3 \cdot d$

Problem 1.3 (4) (1 point)

Let x be an integer. Match the statements below by entering the letter of the corresponding statement on the right.

- | | |
|--|----------------|
| ___ 1. x is greater than or equal to 4 | A. $0 < x$ |
| ___ 2. x is a natural number | B. $x \neq 1$ |
| ___ 3. x is a negative integer | C. $x > 1$ |
| ___ 4. x is not equal to 1 | D. $x \leq -1$ |
| ___ 5. x is greater than 1 | E. $x \geq 4$ |

Problem 1.3 (5) (1 point)

Decide whether the following statements are true or false.

If the statement is false give a counterexample by finding a value for c for which the statements is false.

If the statement is true leave the box for c empty.

(1) For all integers a , b , and c we have $a + (b + c) = a + (b + c)$.

[select: | **The statement is true.** | **The statement is false.**]

If the statement is false, give a counterexample: $a = 6$, $b = 8$, $c =$ __.

(2) For all integers a , b , and c we have $a - (b + c) = (a - b) + c$.

[select: | **The statement is true.** | **The statement is false.**]

If the statement is false, give a counterexample: $a = 6$, $b = 8$, $c =$ __

(3) If a , b , and c are integers then $a - (b - c) = (a - b) - c$.

[select: | **The statement is true.** | **The statement is false.**]

If the statement is false, give a counterexample: $a = 6$, $b = 8$, $c =$ __

(4) If a , b and c are integers then $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

[select: | **The statement is true.** | **The statement is false.**]

If the statement is false, give a counterexample: $a = 6, b = 8, c = \underline{\hspace{1cm}}$.

Problem 1.3 (6) (1 point)

Decide whether the following statements are true or false.

If the statement is false give a counterexample by finding value for the variable for which the statement is false.

if statement is true leave the box empty.

(1) For all integers a and b we have $a - b = b - a$.

[select: | **The statement is true.** | **The statement is false.**]

If the statement is false, give a counterexample: $a = 4, b = \underline{\hspace{1cm}}$

(2) For all integers a, b , and c we have $a - (b + c) = (a - b) + c$.

[select: | **The statement is true.** | **The statement is false.**]

If the statement is false, give a counterexample: $a = 4, b = 5, c = \underline{\hspace{1cm}}$

(3) For all integers a, b , and c we have $a \cdot (b + c) = a \cdot b + a \cdot c$.

[select: | **The statement is true.** | **The statement is false.**]

If the statement is false, give a counterexample: $a = \underline{\hspace{1cm}}, b = 5, c = 4$.

Problem 1.3 (7) (1 point)

The additive inverse of 14876 is .

Problem 1.3 (8) (1 point)

Answer each of the following questions by T (for true) or F (for false).

If you answer true you are saying that the equation is true for all integers a, b , and c .

If you find working with letters confusing you can test your ideas by checking the equations for some special values, such as $a = 3, b = 4$, and $c = 5$. If you do not get equality for such a special case, the equation cannot be true for all integers a, b , and c . If it is true for some special values, it still could be false in general. For example, all these equations are true for $a = 0, b = 0$, and $c = 0$.

i) $(a + b) + c = a + (b + c)$ is .

ii) $(a - b) - c = a - (b - c)$ is ____.

iii) $(a - b) + c = a - (b + c)$ is ____.

iv) $(a + b) - c = a + (b - c)$ is ____.

v) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ is ____.

Problem 1.3 (9) (1 point)

Match the statements below by entering the letter of the corresponding name of the property on the right.

- | | |
|---|-------------------------------------|
| ___ 1. For all integers a and b we have $a \cdot b = b \cdot a$. | A. Distributive property |
| ___ 2. For all integers a , b , and c we have $a + (b + c) = (a + b) + c$.
multiplication | B. Commutative property of |
| ___ 3. For all integers a , b , and c we have $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$. | C. Associative property of addition |

Problem 1.3 (10) (1 point)

Decide whether the following statements are true or false.

If the statement is true provide a witness, that is, a value for the variable a for which the statement is true.

If the statement is false leave the field for the variable empty.

(1) There exists an integer a such that $a \cdot 5 = 1$.

[select: | **The statement is true.** | **The statement is false.**]

If the statement is true, give an integer for which it is true: $a =$ ____

(2) There exists a natural number a such that $14 \cdot a = 1$.

[select: | **The statement is true.** | **The statement is false.**]

If the statement is true, give a natural number for which it is true: $a =$ ____

(3) There exists a natural number a such that $a < 0$.

[select: | **The statement is true.** | **The statement is false.**]

If the statement is true, give a natural number for which it is true: $a =$ ____

(4) There exists an integer a such that $2 > a$.

[select: | **The statement is true.** | **The statement is false.**]

If the statement is true, give an integer for which it is true: $a = \underline{\hspace{1cm}}$

Problem 1.3 (11) (1 point)

Let a and b be integers.

Match the expressions to the terminology by entering the correct letters from the left column in the right column.

___ 1. $a - b$

A. the sum of a and b

___ 2. $a + b$

B. the square of a

___ 3. $a \cdot b$

C. the difference of a and b

___ 4. a^2

D. the product of a and b

Solutions

Problem 1.3 (1) *Correct Answers:*

Hint: Knowing the properties of addition and multiplication can save some work.

Correct Answers:

- 21
- 21
- 4
- -4
- 21
- 21
- 44
- 44
- 10
- -12

Problem 1.3 (2) *Correct Answers:*

- -24
- 12
- -8
- 11

Problem 1.3 (3) *Correct Answers:*

- T
- T
- F
- N

Problem 1.3 (4) *Correct Answers:*

- E
- A
- D
- B
- C

Problem 1.3 (5) *Correct Answers:*

- (1) The statement is true. There is no counterexample.
- (2) The statement is false.
All integers c except for $c = 0$ yield a counterexample.
For example for $c = 2$ we get

$$a - (b + c) = 6 - (8 + 2) = 6 - 10 = -4$$

and

$$(a - b) + c = (6 - 8) + 2 = -2 + 2 = 0$$

so that

$$a - (b + c) = -4 \neq 0 = (a - b) + c$$

- (3) The statement is false.

All integers c except for $c = 0$ yield a counterexample.

For example for $c = 3$ we get

$$a - (b - c) = 6 - (8 - 3) = 6 - 7 = -1$$

and

$$(a - b) - c = (6 - 8) - 3 = -2 - 3 = -5$$

so that

$$a - (b + c) = -1 \neq -5 = (a - b) - c$$

- (4) The statement is true. There is no counterexample.

Problem 1.3 (6) Correct Answers:

- (1) The statement is false.

All integers b except for $b = 4$ yield a counterexample.

For example for $b = 2$ we get

$$a - b = 4 - 0 = 4$$

and

$$b - a = 0 - 4 = -4$$

so that

$$a - b = 4 \neq -4 = b - a.$$

- (2) The statement is false.

All integers b except for $c = 0$ yield a counterexample.

For example for $c = 5$ we get

$$a - (b + c) = 4 - (5 + 5) = 4 - 10 = -6$$

and

$$(a - b) + c = (4 - 5) + 5 = -1 + 5 = -4$$

so that

$$a - (b + c) = -6 \neq -4 = (a - b) + c.$$

- (3) The statement is true. There is no counterexample.

Problem 1.3 (7) Correct Answers:

Hint: The additive inverse of an integer m is the integer n such that $m + n = 0$.

Correct Answers:

- -14876

Problem 1.3 (8) Correct Answers:

Solution:

i) $(a + b) + c = a + (b + c)$ is called the associative law of addition and is true for any values of a, b , and c .

ii) $(a - b) - c = a - (b - c)$ is false. $(a - b) - c = a - b - c$ but $a - (b - c) = a - b + c$.

This is one of the reasons that one of the rules for order of operations includes evaluating unparenthesized

additions and subtractions from left to right.
We will see more such reasons.

iii) $(a - b) + c = a - (b + c)$ is false. $(a - b) + c = a - b + c$ but $a - (b + c) = a - b - c$.

iv) $(a + b) - c = a + (b - c)$ is true since both are equal to $a + b - c$

v) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ is called the associative law of multiplication and is true for all values of a, b , and c .

Correct Answers:

- T
- F
- F
- T
- T

Problem 1.3 (9) *Correct Answers:*

- B
- C
- A

Problem 1.3 (10) *Correct Answers:*

- The Statement is false N/A
- The Statement is false N/A
- The Statement is false N/A
- The statement is true 1

Problem 1.3 (11) *Correct Answers:*

- C
- A
- D
- B

1.4 Exponentiation

Problem 1.4 (1) (1 point)

Compute:

$$0^6 = \underline{\hspace{1cm}}$$

$$1^6 = \underline{\hspace{1cm}}$$

$$2^6 = \underline{\hspace{1cm}}$$

$$3^6 = \underline{\hspace{1cm}}$$

$$4^6 = \underline{\hspace{1cm}}$$

$$5^6 = \underline{\hspace{1cm}}$$

Problem 1.4 (2) (1 point)

Compute:

$$4^0 = \underline{\hspace{1cm}}$$

$$4^1 = \underline{\hspace{1cm}}$$

$$4^2 = \underline{\hspace{1cm}}$$

$$4^3 = \underline{\hspace{1cm}}$$

$$4^4 = \underline{\hspace{1cm}}$$

$$4^5 = \underline{\hspace{1cm}}$$

$$4^6 = \underline{\hspace{1cm}}$$

$$4^7 = \underline{\hspace{1cm}}$$

$$4^8 = \underline{\hspace{1cm}}$$

$$4^9 = \underline{\hspace{1cm}}$$

$$4^{10} = \underline{\hspace{1cm}}$$

Problem 1.4 (3) (1 point)

Complete this operation table for exponentiation. In each table cell enter the heading b of the row to the heading n of the column.

b^n	0	1	2	3	4
-2	—	—	—	—	—
-1	—	—	—	—	—
0	1	—	—	—	0
1	—	1	1	—	1
2	—	—	4	—	16

Problem 1.4 (4) (1 point)

Compute $(-7)^4 =$ _____

Problem 1.4 (5) (1 point)

Match the expression that are equal for all integers a and b and all non-negative integers n and m . Enter the letters next to the numbers.

- | | |
|----------------------------|--------------------|
| ___ 1. $(a \cdot b)^n$ | A. a^3 |
| ___ 2. $a \cdot a$ | B. a^2 |
| ___ 3. $(a^n)^m$ | C. a |
| ___ 4. a^0 | D. 1 |
| ___ 5. a^1 | E. $a^n \cdot b^n$ |
| ___ 6. a^{n+m} | F. $a^n \cdot a^m$ |
| ___ 7. $a \cdot a \cdot a$ | G. $a^{n \cdot m}$ |
-

Problem 1.4 (6) (1 point)

Match the expression that are equal by entering the letters next to the numbers.

- | | |
|-------------------------------|--------------------------------|
| ___ 1. 210^{7456} | A. 7456^{210} |
| ___ 2. 7456^1 | B. $14^{7456} \cdot 14^{15}$ |
| ___ 3. $14^{7456+15}$ | C. 1 |
| ___ 4. 7456^0 | D. 7456 |
| ___ 5. $14^{(15 \cdot 7456)}$ | E. $7456 \cdot 7456$ |
| ___ 6. $(7456^{14})^{15}$ | F. $(14^{15})^{7456}$ |
| ___ 7. 7456^2 | G. $15^{7456} \cdot 14^{7456}$ |

Problem 1.4 (7) (1 point)

Use the properties of exponents to simplify the following.

To enter an answer of the form (x^c) you enter the answer in the form x^c , where c is an integer.

$$x^7 \cdot x^{18} = \underline{\hspace{2cm}}$$

Problem 1.4 (8) (1 point)

Use the properties of exponents to simplify the following. Do not evaluate.

The answer will be of the form 3^x . Enter the answer in the form 3^x , where x is an integer.

$$3^6 \cdot 3^2 = \underline{\hspace{2cm}}$$

Problem 1.4 (9) (1 point)

Use the properties of exponents to simplify the following.

Enter the solution in the form 6^x (to express 6 to the x) where x is an integer.

$$(6^6)^6 = \underline{\hspace{2cm}}$$

Problem 1.4 (10) (1 point)

Use the properties of exponents to simplify the following

$$y^{18} \cdot y^{20} = \underline{\hspace{2cm}}$$

The answer will be of the form y^x . Enter the answer in the form y^x , where x is an integer.

Problem 1.4 (11) (1 point)

Use the properties of exponents to simplify the following

$$(y^4)^{11}$$

Example: Enter y^4 as y^4 .

Problem 1.4 (12) (1 point)

Decide whether the following statements are true or false.

If the statement is false give a counterexample.

(i) For all integers a and b we have $(a \cdot b)^2 = b^2 \cdot a^2$.

[select: | **The statement is true.** | **The statement is false.**]

Give a counterexample if the statement is false: $a = 2$, $b =$ _____

(i) For all integers a and b we have $a^1 a^2 = a^3$.

[select: | **The statement is true.** | **The statement is false.**]

Give a counterexample if the statement is false: $a = 2$, $b =$ _____

(iii) For all natural numbers n we have $(2 + 7)^n = 2^n + 7^n$.

[select: | **The statement is true.** | **The statement is false.**]

If the statement is false, give a counterexample: $n =$ _____

Problem 1.4 (13) (1 point)

$\sqrt{4939198588381830^2}$ is: _____

Problem 1.4 (14) (1 point)

$\sqrt{21810637104679422^2}$ is: _____

Solutions

Problem 1.4 (1) *Correct Answers:*

- 0
- 1
- 64
- 729
- 4096
- 15625

Problem 1.4 (2) *Correct Answers:*

- 1
- 4
- 16
- 64
- 256
- 1024
- 4096
- 16384
- 65536
- 262144
- 1048576

Problem 1.4 (3) **Hint:** Let b be an integer and let n be a natural number. The n -th power of b is:

$$b^n := \underbrace{b \cdot b \cdot \dots \cdot b}_{n \text{ copies of } b}.$$

Furthermore we define $b^0 = 1$.

Evaluate the powers to complete the table:

b^n	0	1	2	3	4
-2	$(-2)^0$	$(-2)^1$	$(-2)^2$	$(-2)^3$	$(-2)^4$
-1	$(-1)^0$	$(-1)^1$	$(-1)^2$	$(-1)^3$	$(-1)^4$
0	1	0^1	0^2	0^3	0
1	1^0	1	1	1^3	1
2	2^0	2^1	4	2^3	16

Correct Answers:

b^n	0	1	2	3	4
-2	1	-2	4	-8	16
-1	1	-1	1	-1	1
0	1	0	0	0	0
1	1	1	1	1	1
2	1	2	4	8	16

Problem 1.4 (4) *Correct Answers:*

- 2401

Problem 1.4 (5) *Correct Answers:*

- E
- B
- G
- D
- C
- F
- A

Problem 1.4 (6) *Correct Answers:*

- G
- D
- B
- C
- F
- A
- E

Problem 1.4 (7) *Correct Answers:*

Solution:

We *add* the exponents as follows

$$\begin{aligned}x^7 \cdot x^{18} &= x^{7+18} \\ &= x^{25}\end{aligned}$$

Correct Answers:

- x^{25}

Problem 1.4 (8) *Correct Answers:*

Solution:

We *add* the exponents as follows

$$\begin{aligned}3^6 \cdot 3^2 &= 3^{6+2} \\ &= 3^8\end{aligned}$$

Correct Answers:

- 3^8

Problem 1.4 (9) *Correct Answers:*

Solution:

We *multiply* the exponents as follows

$$\begin{aligned}(6^6)^6 &= 6^{6 \cdot 6} \\ &= 6^{36}\end{aligned}$$

Correct Answers:

- 6^{36}

Problem 1.4 (10) *Correct Answers:*

Solution:

We *add* the exponents as follows

$$\begin{aligned}y^{18} \cdot y^{20} &= y^{18+20} \\ &= y^{38}\end{aligned}$$

Correct Answers:

- y^{38}

Problem 1.4 (11) *Correct Answers:*

Solution:

We *multiply* the exponents as follows

$$\begin{aligned}(y^4)^{11} &= y^{4 \cdot 11} \\ &= y^{44}\end{aligned}$$

Correct Answers:

- y^{44}

Problem 1.4 (12) *Correct Answers:*

- The statement is true. N/A
- The statement is true. N/A
- The statement is false. 1

Problem 1.4 (13) *Correct Answers:*

- 4939198588381830

Problem 1.4 (14) *Correct Answers:*

- 21810637104679422

Chapter 2

Algorithms

1. return
2. if-then
3. let
4. repeat-until
5. Exponentiation Algorithm

2.2 return

Problem 2.2 (1) (1 point)

Complete the algorithm and find the output for the given input values.

Algorithm

Input: [select: | two integers g and h | an integer g | an integer h | nothing]

Output: the product of g and h

(1) **return** g·h

Find the output of the algorithm for the input $g := 8$ and $h := 9$: ____

Find the output of the algorithm for the input $g := 1$ and $h := -2$: ____

Find the output of the algorithm for the input $g := 6$ and $h := 4$: ____

Problem 2.2 (2) (1 point)

Complete the algorithm and find the output for the given input values.

Algorithm

Input: [select: | two integers e and b | an integer e | an integer b | nothing]

Output: the sum of e and b

(1) **return** e+b

Find the output of the algorithm for the input $e := -6$ and $b := -2$: ____

Find the output of the algorithm for the input $e := 7$ and $b := -1$: ____

Find the output of the algorithm for the input $e := 4$ and $b := 2$: ____

Problem 2.2 (3) (1 point)

Complete the algorithm:

Algorithm

Input: an integer i

Output: [select: | the sum of i and f | the difference of i and f | the product of i and f | the negative of i | the integer 29]

(1) **return** -i

Find the output of the algorithm for the input i:=-8: ____

Find the output of the algorithm for the input i:=1: ____

Find the output of the algorithm for the input i:=-10: ____

Problem 2.2 (4) (1 point)

Complete the algorithm:

Algorithm

Input: an integer i

Output: the integer 28

(1) **return** [select: | i+h | i-h | -i | 28]

Find the output of the algorithm for the input i:=-2: ____

Find the output of the algorithm for the input i:=7: ____

Find the output of the algorithm for the input i:=-10: ____

Problem 2.2 (5) (1 point)

Complete the algorithm:

Algorithm

Input: two integers c and h

Output: [select: | the sum of c and h | the difference of c and h | the product of c and h | the negative of c | the integer 3]

(1) **return** c·h

Find the output of the algorithm for the input c:=7 and h:=10 : ____

Find the output of the algorithm for the input c:=18 and h:=19 : ____

Find the output of the algorithm for the input $c:=-1$ and $h:=1$: ____

Solutions

Problem 2.2 (1) *Correct Answers:*

- two integers g and h
 - 72
 - -2
 - 24
-

Problem 2.2 (2) *Correct Answers:*

- two integers e and b
 - -8
 - 6
 - 6
-

Problem 2.2 (3) *Correct Answers:*

- the negative of i
 - 8
 - -1
 - 10
-

Problem 2.2 (4) *Correct Answers:*

- 28
 - 28
 - 28
 - 28
-

Problem 2.2 (5) *Correct Answers:*

- the product of c and h
- 70
- 342
- -1

2.3 if-then

Problem 2.3 (1) (1 point)

Consider the algorithm:

Algorithm

Input: Two integers a and b .

- (1) **if** $a < b$ **then return** a
- (2) **return** b

What does the algorithm return when the input is $a = -30$ and $b = -88$? ____

What does the algorithm return when the input is $a = -55$ and $b = 13$? ____

What does the algorithm return when the input is $a = -51$ and $b = 0$? ____

What is the **Output** of the algorithm ?

- A. The minimum of a and b
- B. The sum of a and b
- C. The maximum of a and b
- D. The absolute value of a
- E. The greatest common divisor of a and b

Problem 2.3 (2) (1 point)

Consider the algorithm:

Algorithm

Input: Two integers a and b .

- (1) **if** $a < b$ **then return** a, b
- (2) **return** b, a

What does the algorithm return when the input is $a = 80$ and $b = 83$? ____

What does the algorithm return when the input is $a = -46$ and $b = -29$? ____

What does the algorithm return when the input is $a = -10$ and $b = 59$? ____

Problem 2.3 (3) (1 point)

Consider the algorithm:

Algorithm

Input: An integer a

- (1) **if** $a < 0$ **then return** a
(2) **return** $-a$

What does the algorithm return when the input is $a = 26$? ____

What does the algorithm return when the input is $a = -16$? ____

What does the algorithm return when the input is $a = -45$? ____

What does the algorithm return when the input is $a = -79$? ____

What does the algorithm return when the input is an integer a ?

- A. The maximum of a and 0.
- B. The negative of the absolute value of a
- C. The integer a
- D. The absolute value of a
- E. The reciprocal of a
- F. The negative of a
- G. The factorial of a

Problem 2.3 (4) (1 point)

Consider the algorithm:

Algorithm

Input: Two integers a and b .

- (1) **if** $a > b$ **then return** a
(2) **return** b

What does the algorithm return when the input is $a = -16$ and $b = 52$? ____

What does the algorithm return when the input is $a = -61$ and $b = -80$? ____

What does the algorithm return when the input is $a = 89$ and $b = -5$? ____

What is the **Output** of the algorithm ?

- A. The absolute value of a
- B. The sum of a and b
- C. The minimum of a and b
- D. The maximum of a and b
- E. The greatest common divisor of a and b

Problem 2.3 (5) (1 point)

Consider the algorithm:

Algorithm

Input: Two integers a and b .

(1) **if** $a > b$ **then return** a
(2) **return** b

What does the algorithm return when the input is $a = -86$ and $b = 3$? ____

What does the algorithm return when the input is $a = 71$ and $b = 52$? ____

What does the algorithm return when the input is $a = -91$ and $b = -70$? ____

What is the **Output** of the algorithm ?

- A. The sum of a and b
- B. The greatest common divisor of a and b
- C. The minimum of a and b
- D. The maximum of a and b
- E. The absolute value of a

Solutions

Problem 2.3 (1) *Correct Answers:*

- -88
 - -55
 - -51
 - A
-

Problem 2.3 (2) *Correct Answers:*

- $80, 83$
 - $-46, -29$
 - $-10, 59$
-

Problem 2.3 (3) *Correct Answers:*

- -26
 - -16
 - -45
 - -79
 - B
-

Problem 2.3 (4) *Correct Answers:*

- 52
 - -61
 - 89
 - D
-

Problem 2.3 (5) *Correct Answers:*

- 3
- 71
- -70
- D

2.4 let

Problem 2.4 (1) (1 point)

Consider the algorithm:

Algorithm

Input: Two integers a and b .

- (1) **let** $c := a - b$
- (2) **return** c

What does the algorithm return when the input is $a = 0$ and $b = -5$? ____

What does the algorithm return when the input is $a = -4$ and $b = 1$? ____

What does the algorithm return when the input is $a = 18$ and $b = -6$? ____

What does the algorithm return when the input is $a = 8$ and $b = -7$? ____

Problem 2.4 (2) (1 point)

Consider the algorithm:

Input: An integer a .

- (1) **let** $b := a \cdot a$
- (2) **let** $c := b \cdot b$
- (3) **return** $a \cdot c$

What does the algorithm return when the input is $a = -2$? ____

What does the algorithm return when the input is $a = 0$? ____

What does the algorithm return when the input is $a = 5$? ____

What does the algorithm return when the input is an integer a ?

- A. a^5
- B. a^4
- C. a^6
- D. $4 \cdot a$
- E. a^2
- F. a^8
- G. a^1

Problem 2.4 (3) (1 point)

Consider the algorithm:

Algorithm

Input: An integer a .

- (1) **let** $c := a$
- (2) **let** $c := c + 9$
- (3) **let** $c := c + 4$
- (4) **return** c

What does the algorithm return when the input is $a = -4$? ____

What does the algorithm return when the input is $a = -8$? ____

What does the algorithm return when the input is $a = -4$? ____

What does the algorithm return when the input is $a = 2$? ____

Problem 2.4 (4) (1 point)

Consider the algorithm:

Algorithm

Input: Two integers a and b .

- (1) **let** $c := a + b$
- (2) **let** $d := a \cdot b$
- (3) **let** $e := d - c$
- (4) **return** c

What does the algorithm return when the input is $a = -2$ and $b = 0$? ____

What does the algorithm return when the input is $a = 10$ and $b = 4$? ____

What does the algorithm return when the input is $a = 14$ and $b = -9$? ____

What does the algorithm return when the input is $a = -4$ and $b = -4$? ____

Problem 2.4 (5) (1 point)

Consider the algorithm:

Algorithm

Input: Two integers a and b .

(1) **let** $c := a \cdot b$

(2) **return** c

What does the algorithm return when the input is $a = 2$ and $b = -7$? ____

What does the algorithm return when the input is $a = -4$ and $b = 2$? ____

What does the algorithm return when the input is $a = -4$ and $b = -5$? ____

What does the algorithm return when the input is $a = 1$ and $b = 2$? ____

Solutions

Problem 2.4 (1) *Correct Answers:*

- 5
- -5
- 24
- 15

Problem 2.4 (2) *Correct Answers:*

- -32
- 0
- 3125
- A

Problem 2.4 (3) *Correct Answers:*

- 9
- 5
- 9
- 15

Problem 2.4 (4) *Correct Answers:*

- -2
- 14
- 5
- -8

Problem 2.4 (5) *Correct Answers:*

- -14
- -8
- 20
- 2

2.5 repeat-until

Problem 2.5 (1) (1 point)

Consider the algorithm:

Algorithm

Input: A natural number n

```
(1) let  $c := n$ 
(2) repeat
— (a) let  $c := c + 4$ 
(3) until  $c \geq 25$ 
(5) return  $c$ 
```

What does the algorithm return when the input is $n = 11$? _____

What does the algorithm return when the input is $n = 7$? _____

What does the algorithm return when the input is $n = 6$? _____

Problem 2.5 (2) (1 point)

Consider the following algorithm.

Algorithm **Factorial**

Input: A natural number n

Output: $n!$

```
(1) let  $f := 1$ 
(2) repeat
— (a) let  $f := f \cdot n$ 
— (b) let  $n := n - 1$ 
(3) until  $n = 0$ 
(4) return  $f$ 
```

Now use the algorithm to compute the factorial of $n = 4$.

Input: A natural number $n = \underline{\hspace{1cm}}$.

(1) **let** $f := 1$.

(2) **repeat**
— (a) **let** $f := f \cdot n = \underline{\hspace{1cm}}$

— (b) **let** $n := n - 1 = ___$

(3) Because the statement $n = 1$ is false, the loop is repeated. We continue with step (2).

(2) **repeat**

— (a) **let** $f := f \cdot n = ___$

— (b) **let** $n := n - 1 = ___$

(3) Because the statement $n = 1$ is false, the loop is repeated. We continue with step (2).

(2) **repeat**

— (a) **let** $f := f \cdot n = ___$

— (b) **let** $n := n - 1 = ___$

(3) Because the statement $n = 1$ is true, the loop ends. We continue with step (4).

(4) **return** f

Output: $f = ___$

Problem 2.5 (3) (1 point)

Consider the following sequence of instructions:

Input: A natural number n

(1) **repeat**

— (a) **let** $n := n + 7$

(2) **until** $n < 7$

(3) **return** n

What does this return when the input is a natural number n ?

- A. $-n + 7$
- B. $(7)^n$
- C. The remainder of the division of n by 7.
- D. The difference of the first n natural numbers and 7.
- E. The greatest common divisor of 7 and n
- F. Nothing, it never finishes the computation
- G. $7 \cdot n$

Problem 2.5 (4) (1 point)

Consider the algorithm:

Input: A natural number n

```

(1) let  $c := 0$ 
(2) let  $i := 0$ 
(3) repeat
— (a) let  $i := i + 1$ 
— (b) let  $c := c + i^2$ 
(4) until  $i = n$ 
(5) return  $c$ 

```

What does the algorithm return when the input is $n = 2$? ____

What does the algorithm return when the input is $n = 3$? ____

What does the algorithm return when the input is $n = 5$? ____

What does the algorithm return when the input is a natural number n ?

- A. n^2
- B. The product of the first n natural numbers
- C. $(2 \cdot 3)^n$
- D. The sum of the first n natural numbers.
- E. The sum of the first n squares.
- F. 2^n

Problem 2.5 (5) (1 point)

Consider the algorithm:

Input: A natural number n

```

(1) let  $c := 1$ 
(2) repeat
— (a) let  $c := c \cdot n$ 
— (b) let  $n := n - 1$ 
(3) until  $n = 0$ 
(4) return  $c$ 

```

What does the algorithm return when the input is $n = 2$? _____

What does the algorithm return when the input is $n = 4$? _____

What does the algorithm return when the input is $n = 6$? _____

What does the algorithm return when the input is a natural number n ?

- A. The sum of the first n natural numbers.
- B. $(2 \cdot 3)^n$
- C. The sum of the squares of the first n natural numbers.

- D. 2^n
- E. The product of the first n natural numbers.

Problem 2.5 (6) (1 point)

Consider the algorithm:

Algorithm

Input: A natural number n

```
(1) let  $c := n$ 
(2) repeat
— (a) let  $c := c + 4$ 
(3) until  $c \geq 10$ 
(5) return  $c$ 
```

What does the algorithm return when the input is $n = 5$? _____

What does the algorithm return when the input is $n = 4$? _____

What does the algorithm return when the input is $n = 3$? _____

Problem 2.5 (7) (1 point)

Consider the following sequence of instructions:

Input: A natural number n

```
(1) repeat
— (a) let  $n := n + 6$ 
(2) until  $n < 6$ 
(3) return  $n$ 
```

What does this return when the input is a natural number n ?

- A. The remainder of the division of n by 6.
- B. $-n + 6$
- C. $6 \cdot n$
- D. The greatest common divisor of 6 and n
- E. Nothing, it never finishes the computation
- F. The difference of the first n natural numbers and 6.
- G. $(6)^n$

Solutions

Problem 2.5 (1) *Correct Answers:*

- 27
- 27
- 26

Problem 2.5 (2) *Correct Answers:*

- 4
- 4
- 3
- 12
- 2
- 24
- 1
- 24

Problem 2.5 (3) *Correct Answers:*

- F

Problem 2.5 (4) *Correct Answers:*

- 5
- 14
- 55
- E

Problem 2.5 (5) *Correct Answers:*

- 2
- 24
- 720
- E

Problem 2.5 (6) *Correct Answers:*

- 13
- 12
- 11

Problem 2.5 (7) *Correct Answers:*

- E

2.6 Exponentiation Algorithm

Problem 2.6 (1) (1 point)

Exponentiation

With the exponentiation algorithm find 3^3 .

Input: Base $b := \underline{\hspace{1cm}}$ an exponent $n := \underline{\hspace{1cm}}$.

let $i := 0$ and **let** $c := 1$.

let $i := i + 1 = \underline{\hspace{1cm}}$ and **let** $c := c \cdot 3 = \underline{\hspace{1cm}}$.

let $i := i + 1 = \underline{\hspace{1cm}}$ and **let** $c := c \cdot 3 = \underline{\hspace{1cm}}$.

let $i := i + 1 = \underline{\hspace{1cm}}$ and **let** $c := c \cdot 3 = \underline{\hspace{1cm}}$.

Because the statement $i = 3$ is true, we end the loop.

Output: $c = \underline{\hspace{1cm}}$

Problem 2.6 (2) (1 point)

Consider the algorithm:

Algorithm

Input: A non-negative integer n

(1) **if** $n = 0$ **then return** 1

(2) **let** $c := 1$

(3) **let** $i := 0$

(4) **repeat**

— (a) **let** $i := i + 1$

— (b) **let** $c := c \cdot (-3)$

(5) **until** $i = n$

(6) **return** c

What does the algorithm return when the input is $n = 0$? $\underline{\hspace{1cm}}$

What does the algorithm return when the input is $n = 3$? $\underline{\hspace{1cm}}$

What does the algorithm return when the input is $n = 5$? $\underline{\hspace{1cm}}$

What does the algorithm return when the input is a non-negative integer n ?

- A. $-n - 3$
- B. The remainder of the division of n by -3 .
- C. $(-3) \cdot n$
- D. $(-3)^n$
- E. The difference of the first n natural numbers and -3 .
- F. The greatest common divisor of -3 and n

Problem 2.6 (3) (1 point)

Consider the algorithm:

Algorithm

Input: An integer y and a natural number m

```
(1) if  $y = 1$  then return 1
(2) let  $c := 1$ 
(3) let  $i := 0$ 
(4) repeat
— (a) let  $i := i + 1$ 
— (b) let  $c := c \cdot y$ 
(5) until  $i = m$ 
(6) return  $c$ 
```

What does the algorithm return when the input is $y = 3$ and $m = 4$? ____

What does the algorithm return when the input is $y = 2$ and $m = 3$? ____

What does the algorithm return when the input is $y = 3$ and $m = 3$? ____

What does the algorithm return when the input is an integer y and a natural number m ?

- A. the greatest common divisor of y and m
- B. m to the y -th power
- C. y to the m -th power
- D. the product of y and m
- E. the remainder of the division of y by m
- F. the product of the integers from y to m

Problem 2.6 (4) (1 point)

Consider the algorithm:

Algorithm

Input: A natural number n

```
(1) let  $c := 1$ 
(2) let  $i := 0$ 
(3) repeat
— (a) let  $i := i + 1$ 
— (b) let  $c := c \cdot i$ 
(4) until  $i = n$ 
(5) return  $c$ 
```

What does the algorithm return when the input is $n = 1$? _____

What does the algorithm return when the input is $n = 4$? _____

What does the algorithm return when the input is $n = 5$? _____

What does the algorithm return ?

- A. The sum of the first n natural numbers.
- B. $(2 \cdot 3)^n$
- C. The product of the first n natural numbers.
- D. 2^n

Problem 2.6 (5) (1 point)

Consider the algorithm:

Input: A natural number n

```
(1) let  $c := 1$ 
(2) repeat
— (a) let  $c := c \cdot n$ 
— (b) let  $n := n - 1$ 
(3) until  $n = 0$ 
(4) return  $c$ 
```

What does the algorithm return when the input is $n = 2$? _____

What does the algorithm return when the input is $n = 4$? _____

What does the algorithm return when the input is $n = 6$? _____

What does the algorithm return when the input is a natural number n ?

- A. The sum of the first n natural numbers.
- B. The product of the first n natural numbers.
- C. $(2 \cdot 3)^n$

- D. 2^n
- E. The sum of the squares of the first n natural numbers.

Problem 2.6 (6) (1 point)

Consider the algorithm:

Algorithm

Input: A natural number m

```

(1) if  $m = 0$  then return 1
(2) let  $c := 1$ 
(3) let  $i := 0$ 
(4) repeat
  — (a) let  $i := i + 1$ 
  — (b) let  $c := c \cdot 4$ 
(5) until  $i = m$ 
(6) return  $c$ 

```

What does the algorithm return when the input is $m = 0$? ____

What does the algorithm return when the input is $m = 3$? ____

What does the algorithm return when the input is $m = 5$? ____

What does the algorithm return ?

- A. 4^m
- B. $4 \cdot m$
- C. m^4
- D. $-n$
- E. $m!$
- F. $-4 + m$

Solutions

Problem 2.6 (1) *Correct Answers:*

- 3
- 3
- 1
- 3
- 2
- 9
- 3
- 27
- 27

Problem 2.6 (2) *Correct Answers:*

- 1
- -27
- -243
- D

Problem 2.6 (3) *Correct Answers:*

- 81
- 8
- 27
- C

Problem 2.6 (4) *Correct Answers:*

- 1
- 24
- 120
- C

Problem 2.6 (5) *Correct Answers:*

- 2
- 24
- 720
- B

Problem 2.6 (6) *Correct Answers:*

Correct Answers:

- 1
- 64
- 1024
- A

Chapter 3

Division

1. Quotients and Remainders
2. Division Algorithm
3. Long Division
4. Operation mod
5. Clock Arithmetic
6. ISBN

3.1 Quotients and Remainders

Problem 3.1 (1) (1 point)

Find the quotient and remainder of the division of 27 by 9.

The quotient is ____.

The remainder is ____.

Problem 3.1 (2) (1 point)

Find the quotient and remainder of the division of 25 by 8.

The quotient is ____

The remainder is ____

Let q be the quotient and let r the remainder. Enter thses values in the correct box below.

We have $25 = q \cdot 8 + r = ___ \cdot 8 + ___$.

Problem 3.1 (3) (1 point)

Find the quotient and remainder of the division of 24 by 6.

The quotient is ____

The remainder is ____

Let q be the quotient and let r the remainder. Enter thses values in the correct box below.

We have $24 = q \cdot 6 + r = ___ \cdot 6 + ___$.

Problem 3.1 (4) (1 point)

We have:

$$36 = 4 \cdot 9 + 0$$

Find the quotient and remainder of the division of 36 by 9.

The quotient is ____.

The remainder is ____.

Problem 3.1 (5) (1 point)

We have:

$$228628410848 = 375405 \cdot 609018 + 8558$$

Find the quotient and remainder of the division of 228628410848 by 609018.

$$228628410848 \operatorname{div} 609018 = \underline{\hspace{2cm}}.$$

$$228628410848 \operatorname{mod} 609018 = \underline{\hspace{2cm}}.$$

Problem 3.1 (6) (1 point)

We have:

$$19 = 6 \cdot 3 + 1$$

Find the quotient and remainder of the division of 19 by 3.

The quotient is ____.

The remainder is ____.

Problem 3.1 (7) (1 point)

We have:

$$252125356168 = 388383 \cdot 649166 + 317590$$

Find the quotient and remainder of the division of 252125356168 by 649166.

$$252125356168 \operatorname{div} 649166 = \underline{\hspace{2cm}}.$$

$$252125356168 \operatorname{mod} 649166 = \underline{\hspace{2cm}}.$$

Solutions

Problem 3.1 (1) *Correct Answers:*

- 3
 - 0
-

Problem 3.1 (2) *Correct Answers:*

- 3
 - 1
 - 3
 - 1
-

Problem 3.1 (3) *Correct Answers:*

- 4
 - 0
 - 4
 - 0
-

Problem 3.1 (4) *Correct Answers:*

- 4
 - 0
-

Problem 3.1 (5) *Correct Answers:*

Hint: Let a be an integer and b a natural number.

Suppose $a = b \cdot q + r$ with $0 \leq r < b$. Then the quotient is $q = a \operatorname{div} b$ and the remainder is $r = a \bmod b$.
In this problem $a = 228628410848$ and $b = 609018$.

Correct Answers:

- 375405
 - 8558
-

Problem 3.1 (6) *Correct Answers:*

- 6
 - 1
-

Problem 3.1 (7) *Correct Answers:*

Hint: Let a be an integer and b a natural number.

Suppose $a = b \cdot q + r$ with $0 \leq r < b$. Then the quotient is $q = a \operatorname{div} b$ and the remainder is $r = a \bmod b$.
In this problem $a = 252125356168$ and $b = 649166$.

Correct Answers:

- 388383
- 317590

3.2 Division Algorithm

Problem 3.2 (1) (1 point)

Division

Let $a := 47$ and let $b := 10$. With the division algorithm find $a \operatorname{div} b$ and $r = a \bmod b$.

Input: $a = \underline{\hspace{1cm}}$ and $b = \underline{\hspace{1cm}}$.

let $q := 0$ and **let** $r := a = \underline{\hspace{1cm}}$.

let $q := q + 1 = \underline{\hspace{1cm}}$ and **let** $r := r - 10 = \underline{\hspace{1cm}}$.

let $q := q + 1 = \underline{\hspace{1cm}}$ and **let** $r := r - 10 = \underline{\hspace{1cm}}$.

let $q := q + 1 = \underline{\hspace{1cm}}$ and **let** $r := r - 10 = \underline{\hspace{1cm}}$.

let $q := q + 1 = \underline{\hspace{1cm}}$ and **let** $r := r - 10 = \underline{\hspace{1cm}}$.

Because $r < b$ the loop ends here.

Output: The quotient $q = \underline{\hspace{1cm}}$ and the remainder $r = \underline{\hspace{1cm}}$.

Problem 3.2 (2) (1 point)

Find the quotients and remainders:

$10 \operatorname{div} 4 = \underline{\hspace{1cm}}$ and

$10 \bmod 4 = \underline{\hspace{1cm}}$

$12 \operatorname{div} 6 = \underline{\hspace{1cm}}$ and

$12 \bmod 6 = \underline{\hspace{1cm}}$

$17 \operatorname{div} 8 = \underline{\hspace{1cm}}$ and

$17 \bmod 8 = \underline{\hspace{1cm}}$

$34 \operatorname{div} 2 = \underline{\hspace{1cm}}$ and

$34 \bmod 2 = \underline{\hspace{1cm}}$

$32 \operatorname{div} 2 = \underline{\hspace{1cm}}$ and

$32 \bmod 2 = \underline{\hspace{1cm}}$

Problem 3.2 (3) (1 point)

Find the quotients and remainders:

$6 \text{ div } 7 = \underline{\hspace{1cm}}$ and
 $6 \text{ mod } 7 = \underline{\hspace{1cm}}$

$-32 \text{ div } 8 = \underline{\hspace{1cm}}$ and
 $-32 \text{ mod } 8 = \underline{\hspace{1cm}}$

$19 \text{ div } 5 = \underline{\hspace{1cm}}$ and
 $19 \text{ mod } 5 = \underline{\hspace{1cm}}$

$-27 \text{ div } 3 = \underline{\hspace{1cm}}$ and
 $-27 \text{ mod } 3 = \underline{\hspace{1cm}}$

Problem 3.2 (4) (1 point)

Division

Let $a := 67$ and let $b := 6$. With the division algorithm find $a \text{ div } b$ and $r = a \text{ mod } b$.

Input: $a = \underline{\hspace{1cm}}$ and $b = \underline{\hspace{1cm}}$.

let $q := 0$ and **let** $r := a = \underline{\hspace{1cm}}$.

let $q := q + 1 = \underline{\hspace{1cm}}$ and **let** $r := r - 6 = \underline{\hspace{1cm}}$.

let $q := q + 1 = \underline{\hspace{1cm}}$ and **let** $r := r - 6 = \underline{\hspace{1cm}}$.

let $q := q + 1 = \underline{\hspace{1cm}}$ and **let** $r := r - 6 = \underline{\hspace{1cm}}$.

let $q := q + 1 = \underline{\hspace{1cm}}$ and **let** $r := r - 6 = \underline{\hspace{1cm}}$.

let $q := q + 1 = \underline{\hspace{1cm}}$ and **let** $r := r - 6 = \underline{\hspace{1cm}}$.

let $q := q + 1 = \underline{\hspace{1cm}}$ and **let** $r := r - 6 = \underline{\hspace{1cm}}$.

let $q := q + 1 = \underline{\hspace{1cm}}$ and **let** $r := r - 6 = \underline{\hspace{1cm}}$.

let $q := q + 1 = \underline{\hspace{1cm}}$ and **let** $r := r - 6 = \underline{\hspace{1cm}}$.

let $q := q + 1 = \underline{\hspace{1cm}}$ and **let** $r := r - 6 = \underline{\hspace{1cm}}$.

let $q := q + 1 = \underline{\hspace{1cm}}$ and **let** $r := r - 6 = \underline{\hspace{1cm}}$.

let $q := q + 1 = \underline{\hspace{1cm}}$ and **let** $r := r - 6 = \underline{\hspace{1cm}}$.

Because $r < b$ the loop ends here.

Output: The quotient $q = \underline{\hspace{1cm}}$ and the remainder $r = \underline{\hspace{1cm}}$.

Problem 3.2 (5) (1 point)

Division

Let $a := -77$ and let $b := 14$. With the division algorithm find $a \operatorname{div} b$ and $r = a \bmod b$.

Input: $a = \underline{\hspace{1cm}}$ and $b = \underline{\hspace{1cm}}$.

let $q := 0$ and **let** $r := a = \underline{\hspace{1cm}}$.

let $q := q - 1 = \underline{\hspace{1cm}}$ and **let** $r := r + 14 = \underline{\hspace{1cm}}$.

let $q := q - 1 = \underline{\hspace{1cm}}$ and **let** $r := r + 14 = \underline{\hspace{1cm}}$.

let $q := q - 1 = \underline{\hspace{1cm}}$ and **let** $r := r + 14 = \underline{\hspace{1cm}}$.

let $q := q - 1 = \underline{\hspace{1cm}}$ and **let** $r := r + 14 = \underline{\hspace{1cm}}$.

let $q := q - 1 = \underline{\hspace{1cm}}$ and **let** $r := r + 14 = \underline{\hspace{1cm}}$.

let $q := q - 1 = \underline{\hspace{1cm}}$ and **let** $r := r + 14 = \underline{\hspace{1cm}}$.

Because $r > 0$ the loop ends here.

Output: The quotient $q = \underline{\hspace{1cm}}$ and the remainder $r = \underline{\hspace{1cm}}$.

Problem 3.2 (6) (1 point)

Division

Let $a := 92$ and let $b := 26$. With the division algorithm find $a \operatorname{div} b$ and $r = a \bmod b$.

Input: $a = \underline{\hspace{1cm}}$ and $b = \underline{\hspace{1cm}}$.

let $q := 0$ and **let** $r := a = \underline{\hspace{1cm}}$.

let $q := q + 1 = \underline{\hspace{1cm}}$ and **let** $r := r - 26 = \underline{\hspace{1cm}}$.

let $q := q + 1 = \underline{\hspace{1cm}}$ and **let** $r := r - 26 = \underline{\hspace{1cm}}$.

let $q := q + 1 = \underline{\hspace{1cm}}$ and **let** $r := r - 26 = \underline{\hspace{1cm}}$.

Because $r < b$ the loop ends here.

Output: The quotient $q = \underline{\hspace{1cm}}$ and the remainder $r = \underline{\hspace{1cm}}$.

Problem 3.2 (7) (1 point)

Consider the algorithm:

Algorithm

Input: A natural number n and a natural number m

```
(1) if  $n < m$  then return  $n$ 
(2) repeat
— (a) let  $n := n - m$ ,
(3) until  $n < m$ 
(4) return  $n$ 
```

What does the algorithm return when the input is $n := 4$ and $m := 2$? $\underline{\hspace{1cm}}$

What does the algorithm return when the input is $n := 4$ and $m := 2$? $\underline{\hspace{1cm}}$

What does the algorithm return when the input is $n := 6$ and $m := 2$? $\underline{\hspace{1cm}}$

What does the algorithm compute ?

- A. $-n + m$
- B. The quotient of the division of n by m .
- C. $(m)^n$
- D. The remainder of the division of n by m .
- E. $m \cdot n$
- F. The difference of the sum of the first n natural numbers and m .

Problem 3.2 (8) (1 point)

Consider the algorithm:

Algorithm

Input: A natural number n

```
(1) let  $c := 0$ 
(2) if  $n < 2$  then return  $c$ 
(3) repeat
— (a) let  $n := n - 2$ 
— (b) let  $c := c + 1$ 
```

- (4) **until** $n < 2$
 (5) **return** c

What does the algorithm return when the input is $n := 4$? ____

What does the algorithm return when the input is $n := 5$? ____

What does the algorithm return when the input is $n := 6$? ____

What does the algorithm return when the input is $n := 13$? ____

What does the algorithm return ?

- A. $2 \cdot n$
- B. $(2)^n$
- C. The remainder of the division of n by 2.
- D. The difference of the sum of the first n natural numbers and 2.
- E. The quotient of the division of n by 2.
- F. $-n + 2$

Problem 3.2 (9) (1 point)

Consider the division algorithm:

Algorithm

Input: A natural number n and a natural number m

Output: A natural number q and a natural number r such that $qm + r = n$ and $0 \leq r < m$.

- (1) **if** $n < m$ **then return** $0, n$
 (2) **let** $q := 0$
 (4) **let** $r := n$
 (4) **repeat**
 — (a) **let** $r := r - m$
 — (b) **let** $q := q + 1$
 (5) **until** $r < m$
 (6) **return** q, r

What does the algorithm return when the input is $n := 3$ and $m := 2$?
 $q = \underline{\hspace{1cm}}$ and $r = \underline{\hspace{1cm}}$

What does the algorithm return when the input is $n := 5$ and $m := 3$?
 $q = \underline{\hspace{1cm}}$ and $r = \underline{\hspace{1cm}}$

What does the algorithm return when the input is $n := 13$ and $m := 5$?
 $q = \underline{\hspace{1cm}}$ and $r = \underline{\hspace{1cm}}$

What does the algorithm return when the input is $n := 7$ and $m := 2$?
 $q = \underline{\hspace{1cm}}$ and $r = \underline{\hspace{1cm}}$

Problem 3.2 (10) (1 point)

Consider the algorithm:

Algorithm

Input: A natural number n

(1) **if** $n < 5$ **then return** n
(2) **repeat**
— (a) **let** $n := n - 5$,
(3) **until** $n < 5$
(4) **return** n

What does the algorithm return when the input is $n := 5$? $\underline{\hspace{1cm}}$
What does the algorithm return when the input is $n := 7$? $\underline{\hspace{1cm}}$
What does the algorithm return when the input is $n := 15$? $\underline{\hspace{1cm}}$
What does the algorithm return when the input is $n := 33$? $\underline{\hspace{1cm}}$

What does the algorithm return ?

- A. $-n + 5$
- B. The remainder of the division of n by 5.
- C. The difference of the first n natural numbers and 5.
- D. $(5)^n$
- E. The quotient of the division of n by 5.
- F. $5 \cdot n$

Problem 3.2 (11) (1 point)

Let a be an integer and let b be a natural number. Match the expressions to the terminology.

___ 1. $a - b$

___ 2. $a + b$

___ 3. $a \cdot b$

___ 4. $a \bmod b$

___ 5. a^b

___ 6. $a \operatorname{div} b$

___ 7. $\sqrt{a}$

A. the square root of a

B. the remainder of the division of a by b

C. the quotient of the division of a by b

D. a to the b -th power

E. the sum of a and b

F. the product of a and b

G. the difference of a and b

Problem 3.2 (12) (1 point)

If a is the integer such that

$$a \operatorname{div} 50 = 9$$

and

$$a \bmod 50 = 27.$$

Then $a =$ ___

Problem 3.2 (13) (1 point)

Find the quotient and remainder:

$$-8 \operatorname{div} 71 = ___$$

$$-8 \bmod 71 = ___$$

Problem 3.2 (14) (1 point)

Find the quotient and remainder:

$$70 \operatorname{div} 24 = \underline{\hspace{1cm}}$$

$$70 \operatorname{mod} 24 = \underline{\hspace{1cm}}$$

Solutions

Problem 3.2 (1) *Correct Answers:*

- 47
- 10
- 47
- 1
- 37
- 2
- 27
- 3
- 17
- 4
- 7
- 4
- 7

Problem 3.2 (2) *Correct Answers:*

- 2
- 2
- 2
- 0
- 2
- 1
- 17
- 0
- 16
- 0

Problem 3.2 (3) *Correct Answers:*

- 0
- 6
- -4
- 0
- 3
- 4
- -9
- 0

Problem 3.2 (4) *Correct Answers:*

- 67
- 6
- 67
- 1
- 61
- 2

- 55
- 3
- 49
- 4
- 43
- 5
- 37
- 6
- 31
- 7
- 25
- 8
- 19
- 9
- 13
- 10
- 7
- 11
- 1
- 11
- 1

Problem 3.2 (5) *Correct Answers:*

- -77
- 14
- -77
- -1
- -63
- -2
- -49
- -3
- -35
- -4
- -21
- -5
- -7
- -6
- 7
- -6
- 7

Problem 3.2 (6) *Correct Answers:*

- 92
- 26
- 92
- 1
- 66

- 2
- 40
- 3
- 14
- 3
- 14

Problem 3.2 (7) *Correct Answers:*

- 0
- 0
- 0
- D

Problem 3.2 (8) *Correct Answers:*

- 2
- 2
- 3
- 6
- E

Problem 3.2 (9) *Correct Answers:*

- 1
- 1
- 1
- 2
- 2
- 3
- 3
- 1

Problem 3.2 (10) *Correct Answers:*

- 0
- 2
- 0
- 3
- B

Problem 3.2 (11) *Correct Answers:*

- G
- E
- F
- B
- D
- C
- A

Problem 3.2 (12) *Correct Answers:*

Hint: Let a be an integer and b a natural number.

Suppose $a = b \cdot q + r$ with $0 \leq r < b$. Then we write $q = a \operatorname{div} b$ and $r = a \bmod b$.

In this problem $b = 50$ and $q = a \operatorname{div} 50 = 9$ and $r = a \bmod 50 = 27$. Now find a .

Correct Answers:

- 477

Problem 3.2 (13) *Correct Answers:*

- -1
- 63

Problem 3.2 (14) *Correct Answers:*

- 2
- 22

3.3 Long Division

Problem 3.3 (1) (1 point)

Find the quotient and remainder of the division of 5349 by 73. Give at least one digit after the decimal point.

With a calculator compute $d := 5349 \div 73 = \underline{\hspace{1cm}}$.

The quotient q is the integer to the left of d on the number line. Thus $q = \underline{\hspace{1cm}}$.

The remainder is $r := 5349 - (73 \cdot q) = \underline{\hspace{1cm}}$.

So we have found that $5349 \operatorname{div} 73 = \underline{\hspace{1cm}}$ and $5349 \operatorname{mod} 73 = \underline{\hspace{1cm}}$.

Problem 3.3 (2) (1 point)

Find the quotient and remainder of the division of -6367 by 2612. Give at least one digit after the decimal point.

With a calculator compute $d := -6367 \div 2612 = \underline{\hspace{1cm}}$.

The quotient q is the integer to the left of d on the number line. Thus $q = \underline{\hspace{1cm}}$.

The remainder is $r := -6367 - (2612 \cdot q) = \underline{\hspace{1cm}}$.

So we have found that $-6367 \operatorname{div} 2612 = \underline{\hspace{1cm}}$ and $-6367 \operatorname{mod} 2612 = \underline{\hspace{1cm}}$.

Problem 3.3 (3) (1 point)

Find the quotients and remainders:

$4550 \operatorname{div} 678 = \underline{\hspace{1cm}}$ and

$4550 \operatorname{mod} 678 = \underline{\hspace{1cm}}$

$4733 \operatorname{div} 560 = \underline{\hspace{1cm}}$ and

$4733 \operatorname{mod} 560 = \underline{\hspace{1cm}}$

$2241 \operatorname{div} 695 = \underline{\hspace{1cm}}$ and

$2241 \operatorname{mod} 695 = \underline{\hspace{1cm}}$

$1567 \operatorname{div} 697 = \underline{\hspace{1cm}}$ and

$1567 \operatorname{mod} 697 = \underline{\hspace{1cm}}$

$2764 \operatorname{div} 686 = \underline{\hspace{1cm}}$ and

$2764 \operatorname{mod} 686 = \underline{\hspace{1cm}}$

Problem 3.3 (4) (1 point)

Find the quotients and remainders:

$$59880 \operatorname{div} 1997 = \underline{\hspace{1cm}} \text{ and}$$

$$59880 \operatorname{mod} 1997 = \underline{\hspace{1cm}}$$

$$-98474 \operatorname{div} 1070 = \underline{\hspace{1cm}} \text{ and}$$

$$-98474 \operatorname{mod} 1070 = \underline{\hspace{1cm}}$$

$$54702 \operatorname{div} 939 = \underline{\hspace{1cm}} \text{ and}$$

$$54702 \operatorname{mod} 939 = \underline{\hspace{1cm}}$$

$$-83287 \operatorname{div} 1288 = \underline{\hspace{1cm}} \text{ and}$$

$$-83287 \operatorname{mod} 1288 = \underline{\hspace{1cm}}$$

Problem 3.3 (5) (1 point)

Find the quotient and remainder:

$$-30 \operatorname{div} 78 = \underline{\hspace{1cm}}$$

$$-30 \operatorname{mod} 78 = \underline{\hspace{1cm}}$$

Problem 3.3 (6) (1 point)

Find the quotient and remainder:

$$66 \operatorname{div} 49 = \underline{\hspace{1cm}}$$

$$66 \operatorname{mod} 49 = \underline{\hspace{1cm}}$$

Solutions

Problem 3.3 (1) *Correct Answers:*

- 73.2739726027397
- 73
- 20
- 73
- 20

Problem 3.3 (2) *Correct Answers:*

- -2.43759571209801
- -3
- 1469
- -3
- 1469

Problem 3.3 (3) *Correct Answers:*

- 6
- 482
- 8
- 253
- 3
- 156
- 2
- 173
- 4
- 20

Problem 3.3 (4) *Correct Answers:*

- 29
- 1967
- -93
- 1036
- 58
- 240
- -65
- 433

Problem 3.3 (5) *Correct Answers:*

- -1
- 48

Problem 3.3 (6) *Correct Answers:*

- 1
- 17

3.4 Operation mod

Problem 3.4 (1) (1 point)

Compute:

$$0 \bmod 6 = \underline{\hspace{1cm}}$$

$$1 \bmod 6 = \underline{\hspace{1cm}}$$

$$2 \bmod 6 = \underline{\hspace{1cm}}$$

$$3 \bmod 6 = \underline{\hspace{1cm}}$$

$$4 \bmod 6 = \underline{\hspace{1cm}}$$

$$5 \bmod 6 = \underline{\hspace{1cm}}$$

$$6 \bmod 6 = \underline{\hspace{1cm}}$$

$$7 \bmod 6 = \underline{\hspace{1cm}}$$

$$8 \bmod 6 = \underline{\hspace{1cm}}$$

$$9 \bmod 6 = \underline{\hspace{1cm}}$$

$$10 \bmod 6 = \underline{\hspace{1cm}}$$

$$11 \bmod 6 = \underline{\hspace{1cm}}$$

$$12 \bmod 6 = \underline{\hspace{1cm}}$$

$$13 \bmod 6 = \underline{\hspace{1cm}}$$

Problem 3.4 (2) (1 point)

Compute $136 \bmod 182 = \underline{\hspace{2cm}}$

Problem 3.4 (3) (1 point)

Compute:

$$0 \bmod 5 = \underline{\hspace{1cm}} \text{ and } 0 \bmod 6 = \underline{\hspace{1cm}}$$

$$1 \bmod 5 = \underline{\hspace{1cm}} \text{ and } 1 \bmod 6 = \underline{\hspace{1cm}}$$

$$2 \bmod 5 = \underline{\hspace{1cm}} \text{ and } 2 \bmod 6 = \underline{\hspace{1cm}}$$

$$3 \bmod 5 = \underline{\hspace{1cm}} \text{ and } 3 \bmod 6 = \underline{\hspace{1cm}}$$

$$4 \bmod 5 = \underline{\hspace{1cm}} \text{ and } 4 \bmod 6 = \underline{\hspace{1cm}}$$

$$5 \bmod 5 = \underline{\hspace{1cm}} \text{ and } 5 \bmod 6 = \underline{\hspace{1cm}}$$

$$6 \bmod 5 = \underline{\hspace{1cm}} \text{ and } 6 \bmod 6 = \underline{\hspace{1cm}}$$

$$7 \bmod 5 = \underline{\hspace{1cm}} \text{ and } 7 \bmod 6 = \underline{\hspace{1cm}}$$

$$8 \bmod 5 = \underline{\hspace{1cm}} \text{ and } 8 \bmod 6 = \underline{\hspace{1cm}}$$

$$9 \bmod 5 = \underline{\hspace{1cm}} \text{ and } 9 \bmod 6 = \underline{\hspace{1cm}}$$

$$10 \bmod 5 = \underline{\hspace{1cm}} \text{ and } 10 \bmod 6 = \underline{\hspace{1cm}}$$

$$11 \bmod 5 = \underline{\hspace{1cm}} \text{ and } 11 \bmod 6 = \underline{\hspace{1cm}}$$

Problem 3.4 (4) (1 point)

Compute:

$$0 \bmod 5 = \underline{\hspace{1cm}} \text{ and } 0 \bmod 3 = \underline{\hspace{1cm}}$$

$$1 \bmod 5 = \underline{\hspace{1cm}} \text{ and } 1 \bmod 3 = \underline{\hspace{1cm}}$$

$$2 \bmod 5 = \underline{\hspace{1cm}} \text{ and } 2 \bmod 3 = \underline{\hspace{1cm}}$$

$$3 \bmod 5 = \underline{\hspace{1cm}} \text{ and } 3 \bmod 3 = \underline{\hspace{1cm}}$$

$$4 \bmod 5 = \underline{\hspace{1cm}} \text{ and } 4 \bmod 3 = \underline{\hspace{1cm}}$$

$$5 \bmod 5 = \underline{\hspace{1cm}} \text{ and } 5 \bmod 3 = \underline{\hspace{1cm}}$$

$$6 \bmod 5 = \underline{\hspace{1cm}} \text{ and } 6 \bmod 3 = \underline{\hspace{1cm}}$$

$$7 \bmod 5 = \underline{\hspace{1cm}} \text{ and } 7 \bmod 3 = \underline{\hspace{1cm}}$$

$$8 \bmod 5 = \underline{\hspace{1cm}} \text{ and } 8 \bmod 3 = \underline{\hspace{1cm}}$$

$$9 \bmod 5 = \underline{\hspace{1cm}} \text{ and } 9 \bmod 3 = \underline{\hspace{1cm}}$$

$$10 \bmod 5 = \underline{\hspace{1cm}} \text{ and } 10 \bmod 3 = \underline{\hspace{1cm}}$$

$$11 \bmod 5 = \underline{\hspace{1cm}} \text{ and } 11 \bmod 3 = \underline{\hspace{1cm}}$$

$$12 \bmod 5 = \underline{\hspace{1cm}} \text{ and } 12 \bmod 3 = \underline{\hspace{1cm}}$$

$$13 \bmod 5 = \underline{\hspace{1cm}} \text{ and } 13 \bmod 3 = \underline{\hspace{1cm}}$$

$$14 \bmod 5 = \underline{\hspace{1cm}} \text{ and } 14 \bmod 3 = \underline{\hspace{1cm}}$$

Find the smallest non-negative integer b such that $b \bmod 5 = 3$ and $b \bmod 3 = 2$.
 $b = \underline{\hspace{1cm}}$

Problem 3.4 (5) (1 point)

The remainder when a is divided by 33 is 6 and the remainder when b is divided by 33 is 10.

That is, $a \bmod 33 = 6$ and $b \bmod 33 = 10$.

Find:

$$(a + a) \bmod 33 = \underline{\hspace{1cm}}$$

$$(a + b) \bmod 33 = \underline{\hspace{1cm}}$$

$$(a \cdot b) \bmod 33 = \underline{\hspace{1cm}}$$

$$(a + 9) \bmod 33 = \underline{\hspace{1cm}}$$

$$(9 \cdot b) \bmod 33 = \underline{\hspace{1cm}}$$

Problem 3.4 (6) (1 point)

The remainder when a is divided by 15 is 5 and the remainder when b is divided by 15 is 10.

That is, $a \bmod 15 = 5$ and $b \bmod 15 = 10$.

Find:

$$(a + a) \bmod 15 = \underline{\hspace{1cm}}$$

$$(a + b) \bmod 15 = \underline{\hspace{1cm}}$$

$$(a \cdot b) \bmod 15 = \underline{\hspace{1cm}}$$

$$(a + 7) \bmod 15 = \underline{\hspace{1cm}}$$

$$(7 \cdot b) \bmod 15 = \underline{\hspace{1cm}}$$

Problem 3.4 (7) (1 point)

Compute these remainders:

$$52 \bmod 19 = \underline{\hspace{1cm}}$$

$$4 \bmod 11 = \underline{\hspace{1cm}}$$

$$197 \bmod 9 = \underline{\hspace{1cm}}$$

$$12 \bmod 23 = \underline{\hspace{1cm}}$$

$$183 \bmod 33 = \underline{\hspace{1cm}}$$

$$76 \bmod 5 = \underline{\hspace{1cm}}$$

Problem 3.4 (8) (1 point)

We can write $2182460683 = \underline{\hspace{1cm}} \cdot 100 + \underline{\hspace{1cm}}$

Hint: Example: $1234567 = 12345 \cdot 100 + 67$

Because $83 \bmod 2 = \underline{\hspace{1cm}}$ we have $2182460683 \bmod 2 = \underline{\hspace{1cm}}$.

Because $83 \bmod 4 = \underline{\hspace{1cm}}$ we have $2182460683 \bmod 4 = \underline{\hspace{1cm}}$.

Because $83 \bmod 5 = \underline{\hspace{1cm}}$ we have $2182460683 \bmod 5 = \underline{\hspace{1cm}}$.

Because $83 \bmod 10 = \underline{\hspace{1cm}}$ we have $2182460683 \bmod 10 = \underline{\hspace{1cm}}$.

Because $83 \bmod 20 = \underline{\hspace{1cm}}$ we have $2182460683 \bmod 20 = \underline{\hspace{1cm}}$.

Because $83 \bmod 25 = \underline{\hspace{1cm}}$ we have $2182460683 \bmod 25 = \underline{\hspace{1cm}}$.

Because $83 \bmod 100 = \underline{\hspace{1cm}}$ we have $2182460683 \bmod 100 = \underline{\hspace{1cm}}$.

Problem 3.4 (9) (1 point)

What is the remainder of 23451638 divided by 5? $\underline{\hspace{1cm}}$

What is the remainder of 23451638 divided by 4? $\underline{\hspace{1cm}}$

Hint: This is easier than it looks. Use that 4 and 5 divide 100.

Problem 3.4 (10) (1 point)

Compute:

$$23210494277064179722 \bmod 2 = \underline{\hspace{1cm}}$$

$$23210494277064179722 \bmod 4 = \underline{\hspace{1cm}}$$

$$23210494277064179722 \bmod 5 = \underline{\hspace{1cm}}$$

$$23210494277064179722 \bmod 10 = \underline{\hspace{1cm}}$$

$$23210494277064179722 \bmod 20 = \underline{\hspace{1cm}}$$

$$23210494277064179722 \bmod 25 = \underline{\hspace{1cm}}$$

$$23210494277064179722 \bmod 100 = \underline{\hspace{1cm}}$$

$$23210494277064179722 \bmod 1000 = \underline{\hspace{1cm}}$$

$$23210494277064179722 \bmod 10000 = \underline{\hspace{1cm}}$$

Problem 3.4 (11) (1 point)

Compute:

$$10249838952446438118 \bmod 10 = \underline{\hspace{1cm}}$$

$$10249838952446438118 \bmod 100 = \underline{\hspace{1cm}}$$

$$10249838952446438118 \bmod 1000 = \underline{\hspace{1cm}}$$

$$10249838952446438118 \bmod 10000 = \underline{\hspace{1cm}}$$

$$10249838952446438118 \bmod 100000 = \underline{\hspace{1cm}}$$

$$10249838952446438118 \bmod 1000000 = \underline{\hspace{1cm}}$$

Solutions

Problem 3.4 (1) *Correct Answers:*

- 0
- 1
- 2
- 3
- 4
- 5
- 0
- 1
- 2
- 3
- 4
- 5
- 0
- 1

Problem 3.4 (2) *Correct Answers:*

- 136

Problem 3.4 (3) *Correct Answers:*

- 0
- 0
- 1
- 1
- 2
- 2
- 3
- 3
- 4
- 4
- 0
- 5
- 1
- 0
- 2
- 1
- 3
- 2
- 4
- 3
- 0
- 4
- 1
- 5

Problem 3.4 (4) *Correct Answers:*

- 0
- 0
- 1
- 1
- 2
- 2
- 3
- 0
- 4
- 1
- 0
- 2
- 1
- 0
- 2
- 1
- 3
- 2
- 4
- 0
- 0
- 1
- 1
- 2
- 2
- 0
- 3
- 1
- 4
- 2
- 8

Problem 3.4 (5) *Correct Answers:*

- 12
- 16
- 27
- 15
- 24

Problem 3.4 (6) *Correct Answers:*

- 10
- 0
- 5
- 12

- 10

Problem 3.4 (7) *Correct Answers:*

- 14
- 4
- 8
- 12
- 18
- 1

Problem 3.4 (8) *Correct Answers:*

Hint: In the following each ? can be any number from 0 to 9.

We have

$$2182460683 \bmod 10 = 3 \bmod 10$$

Thus, because 2 and 5 divide 10, also

$$2182460683 \bmod 2 = 3 \bmod 2 \text{ and}$$

$$2182460683 \bmod 5 = 3 \bmod 5$$

Similarly

$$2182460683 \bmod 100 = 83 \bmod 100$$

Thus, because 4 and 20 and 25 divide 100, also

$$2182460683 \bmod 4 = 83 \bmod 4 \text{ and}$$

$$2182460683 \bmod 20 = 83 \bmod 20 \text{ and}$$

$$2182460683 \bmod 25 = 83 \bmod 25.$$

Correct Answers:

- 21824606
- 83
- 1
- 1
- 3
- 3
- 3
- 3
- 3
- 3
- 3
- 3
- 3
- 8
- 8

- 83
- 83

Problem 3.4 (9) *Correct Answers:*

Solution:

This problem can be greatly simplified by looking only at the last two digits. Note that $23451638 = 23451600 + 38$. It should be clear that $5|23451600$ since $5|100$ and $100|23451600$. Thus we need only look at 38.

$$38 = 7 \cdot 5 + 3$$

By the same logic above, we need only look at the remainder of 38 divided by 4.

$$38 = 9 \cdot 4 + 2$$

Correct Answers:

- 3
- 2

Problem 3.4 (10) *Correct Answers:*

Hint: In the following each ? can be any number from 0 to 9.

We have

$$23210494277064179722 \bmod 10 = 2 \bmod 10$$

Thus, because 2 and 5 divide 10, also

$$23210494277064179722 \bmod 2 = 2 \bmod 2 \text{ and}$$

$$23210494277064179722 \bmod 5 = 2 \bmod 5$$

Similarly

$$23210494277064179722 \bmod 100 = 22 \bmod 100$$

Thus, because 4 and 20 and 25 divide 100, also

$$23210494277064179722 \bmod 4 = 22 \bmod 4 \text{ and}$$

$$23210494277064179722 \bmod 20 = 22 \bmod 20 \text{ and}$$

$$23210494277064179722 \bmod 25 = 22 \bmod 25.$$

Correct Answers:

- 0
- 2
- 2
- 2
- 2
- 22
- 22

- 722
- 9722

Problem 3.4 (11) *Correct Answers:*

Hint: We have

$$10249838952446438118 \bmod 10 = 8 \bmod 10$$

and

$$10249838952446438118 \bmod 100 = 18 \bmod 100$$

Correct Answers:

- 8
- 18
- 118
- 8118
- 38118
- 438118

3.5 Clock Arithmetic

Problem 3.5 (1) (1 point)

We use the 24 hour clock. Assume it is 3 p.m. What time will it be 55 hours from now ?

[select: | **12 a.m** | **1 a.m** | **2 a.m** | **3 a.m** | **4 a.m** | **5 a.m** | **6 a.m** | **7 a.m** | **8 a.m** | **9 a.m** | **10 a.m** | **11 a.m** | **12 p.m** | **1 p.m** | **2 p.m** | **3 p.m** | **4 p.m** | **5 p.m** | **6 p.m** | **7 p.m** | **8 p.m** | **9 p.m** | **10 p.m** | **11 p.m**]

Problem 3.5 (2) (1 point)

We use the 12 hour clock. Assume it is 3 o'clock. What time will it be 79 hours from now ?

[select: | **12 o'clock** | **1 o'clock** | **2 o'clock** | **3 o'clock** | **4 o'clock** | **5 o'clock** | **6 o'clock** | **7 o'clock** | **8 o'clock** | **9 o'clock** | **10 o'clock** | **11 o'clock**]

Problem 3.5 (3) (1 point)

We use the 12 hour clock. Assume it is 4 o'clock. What time will it be 12 hours from now ?

[select: | **12 o'clock** | **1 o'clock** | **2 o'clock** | **3 o'clock** | **4 o'clock** | **5 o'clock** | **6 o'clock** | **7 o'clock** | **8 o'clock** | **9 o'clock** | **10 o'clock** | **11 o'clock**]

Problem 3.5 (4) (1 point)

Assume it is December. What month will it be 92 months from now ?

[select: | **January** | **February** | **March** | **April** | **May** | **June** | **July** | **August** | **September** | **October** | **November** | **December**]

Problem 3.5 (5) (1 point)

We use the 24 hour clock. Assume it is 14:00 hours. What time will it be 65 hours from now ?

[select: | **0:00 hours** | **1:00 hours** | **2:00 hours** | **3:00 hours** | **4:00 hours** | **5:00 hours** | **6:00 hours** | **7:00 hours** | **8:00 hours** | **9:00 hours** | **10:00 hours** | **11:00 hours** | **12:00 hours** | **13:00 hours** | **14:00 hours** | **15:00 hours** | **16:00 hours** | **17:00 hours** | **18:00 hours** | **19:00 hours** | **20:00 hours** | **21:00 hours** | **22:00 hours** | **23:00 hours**]

Problem 3.5 (6) (1 point)

Assume it is October. What month will it be 54 months from now ?

[select: | **January** | **February** | **March** | **April** | **May** | **June** | **July** | **August** | **September** | **October** | **November** | **December**]

Solutions

Problem 3.5 (1) *Correct Answers:*

- 10 p.m

Problem 3.5 (2) *Correct Answers:*

- 10 o'clock

Problem 3.5 (3) *Correct Answers:*

- 4 o'clock

Problem 3.5 (4) *Correct Answers:*

- August

Problem 3.5 (5) *Correct Answers:*

- 7:00 hours

Problem 3.5 (6) *Correct Answers:*

Correct Answers:

- April

3.6 ISBN

Problem 3.6 (1) (1 point)

You are given

$$x_1 - x_2x_3x_4x_5x_6 - x_7x_8x_9 - x_{10}$$

as

$$0 - 03088 - 600 - X.$$

Enter the digits

$$x_1 = __\ x_2 = __\ x_3 = __\ x_4 = __\ x_5 = __\ x_6 = __\ x_7 = __\ x_8 = __\ x_9 = __\ x_{10} = __\$$

Compute

$$C := (x_1 + 2 \cdot x_2 + 3 \cdot x_3 + 4 \cdot x_4 + 5 \cdot x_5 + 6 \cdot x_6 + 7 \cdot x_7 + 8x_8 + 9x_9) \bmod 11$$

$$C = __\$$

If $C = x_{10}$ then we have a valid ISBN-10.

Is $0 - 03088 - 600 - X$ a valid ISBN-10 ?

- A. Yes
- B. No

Problem 3.6 (2) (1 point)

You are given

$$x_1 - x_2x_3x_4x_5x_6 - x_7x_8x_9 - x_{10}$$

as

$$5 - 02590 - 000 - X.$$

Enter the digits

$$x_1 = __\ x_2 = __\ x_3 = __\ x_4 = __\ x_5 = __\ x_6 = __\ x_7 = __\ x_8 = __\ x_9 = __\ x_{10} = __\$$

Compute

$$C := (x_1 + 2 \cdot x_2 + 3 \cdot x_3 + 4 \cdot x_4 + 5 \cdot x_5 + 6 \cdot x_6 + 7 \cdot x_7 + 8x_8 + 9x_9) \bmod 11$$

$$C = __\$$

If $C = x_{10}$ then we have a valid ISBN-10.

Is $5 - 02590 - 000 - X$ a valid ISBN-10 ?

- A. Yes
- B. No

Problem 3.6 (3) (1 point)

You are given

$$x_1 - x_2x_3x_4x_5x_6 - x_7x_8x_9 - x_{10}$$

as

$$1 - 59876 - 842 - 0.$$

Compute

$$z = (1 \cdot x_1 + 2 \cdot x_2 + 3 \cdot x_3 + 4 \cdot x_4 + 5 \cdot x_5 + 6 \cdot x_6 + 7 \cdot x_7 + 8 \cdot x_8 + 9 \cdot x_9) \bmod 11$$

$z = \underline{\hspace{2cm}}$

Now you can answer the question.

Is $1 - 59876 - 842 - 0$ a valid ISBN-10 ?

- A. Yes
- B. No

Problem 3.6 (4) (1 point)

You are given

$$x_1 - x_2x_3x_4x_5x_6 - x_7x_8x_9 - x_{10}$$

as

$$1 - 95294 - 785 - 5.$$

Compute

$$z = (1 \cdot x_1 + 2 \cdot x_2 + 3 \cdot x_3 + 4 \cdot x_4 + 5 \cdot x_5 + 6 \cdot x_6 + 7 \cdot x_7 + 8 \cdot x_8 + 9 \cdot x_9) \bmod 11$$

$z = \underline{\hspace{2cm}}$

Now you can answer the question.

Is $1 - 95294 - 785 - 5$ a valid ISBN-10 ?

- A. No
- B. Yes

Problem 3.6 (5) (1 point)

The first nine digits of an ISBN-10 are

2 – 834 – 10840

We compute

$$\left((1 \cdot \text{---}) + (2 \cdot \text{---}) + (3 \cdot \text{---}) + (4 \cdot \text{---}) + (5 \cdot \text{---}) + (6 \cdot \text{---}) + (7 \cdot \text{---}) + (8 \cdot \text{---}) + (9 \cdot \text{---}) \right) \bmod 11 = \text{---}$$

Thus the tenth digit of the ISBN is ---

Problem 3.6 (6) (1 point)

The first nine digits of an ISBN-10 are

8 – 120 – 08074

We compute

$$\left((1 \cdot \text{---}) + (2 \cdot \text{---}) + (3 \cdot \text{---}) + (4 \cdot \text{---}) + (5 \cdot \text{---}) + (6 \cdot \text{---}) + (7 \cdot \text{---}) + (8 \cdot \text{---}) + (9 \cdot \text{---}) \right) \bmod 11 = \text{---}$$

Thus the tenth digit of the ISBN is ---

Problem 3.6 (7) (1 point)

If the first nine characters of an ISBN-10 are

4 – 695 – 92079

then the tenth character is: ---

Problem 3.6 (8) (1 point)

If the first nine characters of an ISBN-10 are

0 – 400 – 38315

then the tenth character is: ---

Solutions

Problem 3.6 (1) *Correct Answers:*

Hint: If $C = 10$ the 10-th digit of the ISBN should be X .

Correct Answers:

- 0
- 0
- 3
- 0
- 8
- 8
- 6
- 0
- 0
- 10
- 7
- B

Problem 3.6 (2) *Correct Answers:*

Hint: If $C = 10$ the 10-th digit of the ISBN should be X .

Correct Answers:

- 5
- 0
- 2
- 5
- 9
- 0
- 0
- 0
- 0
- 10
- 10
- A

Problem 3.6 (3) *Correct Answers:*

Hint:

$$1 - 59876 - 842 - 0$$

is a valid ISBN when z is equal to its last digit, that is, in our case when $z = 0$ where

$$z = (1 \cdot 1 + 2 \cdot 5 + 3 \cdot 9 + 4 \cdot 8 + 5 \cdot 7 + 6 \cdot 6 + 7 \cdot 8 + 8 \cdot 4 + 9 \cdot 2) \bmod 11.$$

Correct Answers:

- 5
- B

Problem 3.6 (4) Correct Answers:**Hint:**

$$1 - 95294 - 785 - 5$$

is a valid ISBN when z is equal to its last digit, that is, in our case when $z = 5$ where

$$z = (1 \cdot 1 + 2 \cdot 9 + 3 \cdot 5 + 4 \cdot 2 + 5 \cdot 9 + 6 \cdot 4 + 7 \cdot 7 + 8 \cdot 8 + 9 \cdot 5) \bmod 11.$$

Correct Answers:

- 5
- B

Problem 3.6 (5) Correct Answers:**Hint:** Recall that the tenth digit of an ISBN can be 1 or 2 or 3 or 4 or 5 or 6 or 7 or 8 or 9 or X.

Correct Answers:

- 2
- 8
- 3
- 4
- 1
- 0
- 8
- 4
- 0
- 4
- 4

Problem 3.6 (6) Correct Answers:**Hint:** Recall that the tenth digit of an ISBN can be 1 or 2 or 3 or 4 or 5 or 6 or 7 or 8 or 9 or X.

Correct Answers:

- 8
- 1
- 2
- 0
- 0
- 8
- 0
- 7
- 4
- 2
- 2

Problem 3.6 (7) Correct Answers:

- 4

Problem 3.6 (8) Correct Answers:

- 2

Chapter 4

Greatest Common Divisors

1. Divisibility
2. Greatest-Common-Divisors
3. Euclidean-Algorithm
4. Bezouts-Identity

4.1 Divisibility

Problem 4.1 (1) (1 point)

Select all divisors of 195.

- A. 2
- B. 3
- C. 5
- D. 9
- E. 10

Problem 4.1 (2) (1 point)

Select all numbers that are divisible by 20.

- A. 3700
- B. 8005
- C. 923
- D. 5820

Problem 4.1 (3) (1 point)

If $a=b \cdot q$ where a , b , and q are natural numbers, then: (check all that apply)

- A. b is divisible by a
- B. b is a divisor of a
- C. a is divisible by b
- D. a divides b
- E. b is a factor of a

Problem 4.1 (4) (1 point)

Enter T or F depending on whether the statement is a true proposition or not. (You must enter T or F – True and False will not work.)

- ___1. 13 is a divisor of 260
- ___2. 13 is a divisor of 260
- ___3. 13 is a factor of 260
- ___4. 13 is a multiple of 260
- ___5. 13 is a factor of 260
- ___6. 260 is a factor of 13

Problem 4.1 (5) (1 point)

Compute the remainder and complete the statement about divisibility

Because $61 \bmod 14 = \underline{\hspace{1cm}}$ we have that 14 61. [select: | **divides** | **does not divide**]

Because $21 \bmod 2 = \underline{\hspace{1cm}}$ we have that 2 21. [select: | **divides** | **does not divide**]

Because $49 \bmod 5 = \underline{\hspace{1cm}}$ we have that 5 49. [select: | **divides** | **does not divide**]

Because $81 \bmod 11 = \underline{\hspace{1cm}}$ we have that 11 81. [select: | **divides** | **does not divide**]

Because $8 \bmod 20 = \underline{\hspace{1cm}}$ we have that 20 8. [select: | **divides** | **does not divide**]

Because $82 \bmod 18 = \underline{\hspace{1cm}}$ we have that 18 82. [select: | **divides** | **does not divide**]

Solutions

Problem 4.1 (1) *Correct Answers:*

Solution:

Does 2 divide 195?

2 divides all even numbers, so 2 does not divide 195.

Does 3 divide 195?

Add up all digits of 195: $1 + 9 + 5 = 15$. Since 3 does divide 15, 3 does divide 195.

Does 5 divide 195?

5 only divides numbers which end with 5 or 0, so 5 does divide 195.

Does 9 divide 195?

Add up all digits of 195: $1 + 9 + 5 = 15$. Since 9 does not divide 15, 9 does not divide 195.

Does 10 divide 195?

10 only divides numbers which end with 0, so 10 does not divide 195.

So the correct answers are BC.

Correct Answers:

- BC

Problem 4.1 (2) *Correct Answers:*

- AD

Problem 4.1 (3) *Correct Answers:*

- BCE

Problem 4.1 (4) *Correct Answers:*

- T
- T
- T
- F
- T
- F

Problem 4.1 (5) Correct Answers:

- 5
- does not divide
- 1
- does not divide
- 4
- does not divide
- 4
- does not divide
- 8
- does not divide
- 10
- does not divide

4.2 Greatest-Common-Divisors

Problem 4.2 (1) (1 point)

List all of the positive common divisors of 28 and 74: _____

Note: Enter your answers as a comma-separated list. The list of common divisors of 8 and 12 is: 1,2,4

What is the greatest common divisor of 28 and 74 ? ____

Problem 4.2 (2) (1 point)

For each of the following pairs of numbers, find the greatest common divisor. Although the numbers are large finding their greatest common divisor is not too hard. Taking a closer look at both numbers reveals special relationships.

$\gcd(1005812, 1005812) = \underline{\hspace{2cm}}$

$\gcd(1226463, 1) = \underline{\hspace{2cm}}$

$\gcd(2498410, 0) = \underline{\hspace{2cm}}$

$\gcd(0, 1226463) = \underline{\hspace{2cm}}$

$\gcd(430586, 430586) = \underline{\hspace{2cm}}$

$\gcd(1, 2498410) = \underline{\hspace{2cm}}$

$\gcd(1226464, 1226464) = \underline{\hspace{2cm}}$

Problem 4.2 (3) (1 point)

For each of the following pairs of numbers, find the greatest common divisor. Taking a closer look at both numbers reveals special relationships.

$\gcd(7883, 1) = \underline{\hspace{2cm}}$

$\gcd(7883, 0) = \underline{\hspace{2cm}}$

$\gcd(7883, 7884) = \underline{\hspace{2cm}}$

$\gcd(9271, 9271) = \underline{\hspace{2cm}}$

Problem 4.2 (4) (1 point)

For each of the following pairs of numbers, find the greatest common divisor.

$$\gcd(13,0)=\underline{\hspace{2cm}}$$

$$\gcd(13,14)=\underline{\hspace{2cm}}$$

$$\gcd(6,6)=\underline{\hspace{2cm}}$$

$$\gcd(1,5)=\underline{\hspace{2cm}}$$

$$\gcd(6,1)=\underline{\hspace{2cm}}$$

$$\gcd(3,2)=\underline{\hspace{2cm}}$$

$$\gcd(1,5)=\underline{\hspace{2cm}}$$

$$\gcd(0,3)=\underline{\hspace{2cm}}$$

Problem 4.2 (5) (1 point)

For each of the following pairs of numbers, find the greatest common divisor.

$$\gcd(15,16)=\underline{\hspace{2cm}}$$

$$\gcd(10,1)=\underline{\hspace{2cm}}$$

$$\gcd(29,0)=\underline{\hspace{2cm}}$$

$$\gcd(0,10)=\underline{\hspace{2cm}}$$

$$\gcd(7,7)=\underline{\hspace{2cm}}$$

$$\gcd(1,29)=\underline{\hspace{2cm}}$$

$$\gcd(11,10)=\underline{\hspace{2cm}}$$

Problem 4.2 (6) (1 point)

For each of the following pairs of numbers, find the greatest common divisor.

$$\gcd(20,21)=\underline{\hspace{2cm}}$$

$$\gcd(20,1)=\underline{\hspace{2cm}}$$

$$\gcd(21,0)=\underline{\hspace{2cm}}$$

$$\gcd(0,20)=\underline{\hspace{2cm}}$$

$$\gcd(25,25)=\underline{\hspace{2cm}}$$

$$\gcd(1,21)=\underline{\hspace{2cm}}$$

$$\gcd(21,20)=\underline{\hspace{2cm}}$$

Problem 4.2 (7) (1 point)

List all of the positive common divisors of 100 and 120:

Note: Enter your answers as a comma-separated list. The list of common divisors of 8 and 12 is: 1,2,4

What is the greatest common divisor of 100 and 120 ?

Problem 4.2 (8) (1 point)

For all integers a and b we have:

$$\gcd(a \bmod b, b) = [\text{select: } \mid \mathbf{0} \mid \mathbf{1} \mid \mathbf{a} \mid \mathbf{b} \mid \mathbf{a+b} \mid \mathbf{\gcd(a,b)}]$$

$$\gcd(a, 0) = [\text{select: } \mid \mathbf{0} \mid \mathbf{1} \mid \mathbf{a} \mid \mathbf{b} \mid \mathbf{a+b} \mid \mathbf{\gcd(a,b)}]$$

$$\gcd(1, b) = [\text{select: } \mid \mathbf{0} \mid \mathbf{1} \mid \mathbf{a} \mid \mathbf{b} \mid \mathbf{a+b} \mid \mathbf{\gcd(a,b)}]$$

$$\gcd(b+1, b) = [\text{select: } \mid \mathbf{0} \mid \mathbf{1} \mid \mathbf{a} \mid \mathbf{b} \mid \mathbf{a+b} \mid \mathbf{\gcd(a,b)}]$$

$$\gcd(a-b, b) = [\text{select: } \mid \mathbf{0} \mid \mathbf{1} \mid \mathbf{a} \mid \mathbf{b} \mid \mathbf{a+b} \mid \mathbf{\gcd(a,b)}]$$

$$a \bmod b < [\text{select: } \mid \mathbf{0} \mid \mathbf{1} \mid \mathbf{a} \mid \mathbf{b} \mid \mathbf{a+b} \mid \mathbf{\gcd(a,b)}]$$

$$\gcd(b, a) = [\text{select: } \mid \mathbf{0} \mid \mathbf{1} \mid \mathbf{a} \mid \mathbf{b} \mid \mathbf{a+b} \mid \mathbf{\gcd(a,b)}]$$

Solutions

Problem 4.2 (1) *Correct Answers:*

Hint: The common divisors of 28 and 74 are all numbers that divide **both** 28 and 74.

Correct Answers:

- 1, 2
 - 2
-

Problem 4.2 (2) *Correct Answers:*

- 1.00581×10^6
 - 1
 - 2.49841×10^6
 - 1.22646×10^6
 - 430586
 - 1
 - 1.22646×10^6
-

Problem 4.2 (3) *Correct Answers:*

- 1
 - 7883
 - 1
 - 9271
-

Problem 4.2 (4) *Correct Answers:*

- 13
 - 1
 - 6
 - 1
 - 1
 - 1
 - 1
 - 3
-

Problem 4.2 (5) *Correct Answers:*

Hint: Let a and b be integers. Then

$$\gcd(a, b) = \gcd(b, a)$$

$$\gcd(a, a) = a$$

$$\gcd(a+1, a) = 1$$

$$\gcd(1, a) = 1$$

$$\gcd(a, 0) = a$$

Correct Answers:

- 1
- 1
- 29

- 10
- 7
- 1
- 1

Problem 4.2 (6) *Correct Answers:*

Hint: Let a and b be an integers. Then

$$\gcd(a, b) = \gcd(b, a)$$

$$\gcd(a, a) = a$$

$$\gcd(a + 1, a) = 1$$

$$\gcd(1, a) = 1$$

$$\gcd(a, 0) = a$$

Correct Answers:

- 1
- 1
- 21
- 20
- 25
- 1
- 1

Problem 4.2 (7) *Correct Answers:*

Hint: The common divisors of 100 and 120 are all numbers that divide **both** 100 and 120.

Correct Answers:

- 1, 2, 4, 5, 10, 20
- 20

Problem 4.2 (8) *Correct Answers:*

- $\gcd(a, b)$
- a
- 1
- 1
- $\gcd(a, b)$
- b
- $\gcd(a, b)$

4.3 Euclidean-Algorithm

Problem 4.3 (1) (1 point)

Follow these step to compute the greatest common divisor of $a := 52$ and $b := 24$:

let $r := a \bmod b = \underline{\hspace{1cm}}$ and **let** $a := b = \underline{\hspace{1cm}}$ and **let** $b := r = \underline{\hspace{1cm}}$

let $r := a \bmod b = \underline{\hspace{1cm}}$ and **let** $a := b = \underline{\hspace{1cm}}$ and **let** $b := r = \underline{\hspace{1cm}}$

The greatest common divisor of 52 and 24 is $a = \underline{\hspace{1cm}}$

Problem 4.3 (2) (1 point)

Follow these step to compute the greatest common divisor of $a := 41$ and $b := 21$:

let $r := a \bmod b = \underline{\hspace{1cm}}$ and **let** $a := b = \underline{\hspace{1cm}}$ and **let** $b := r = \underline{\hspace{1cm}}$

let $r := a \bmod b = \underline{\hspace{1cm}}$ and **let** $a := b = \underline{\hspace{1cm}}$ and **let** $b := r = \underline{\hspace{1cm}}$

let $r := a \bmod b = \underline{\hspace{1cm}}$ and **let** $a := b = \underline{\hspace{1cm}}$ and **let** $b := r = \underline{\hspace{1cm}}$

The greatest common divisor of 41 and 21 is $a = \underline{\hspace{1cm}}$

Problem 4.3 (3) (1 point)

For each of the following pairs of numbers, find the greatest common divisor.

$\text{gcd}(30,42)=\underline{\hspace{1cm}}$

$\text{gcd}(105,165)=\underline{\hspace{1cm}}$

$\text{gcd}(360,504)=\underline{\hspace{1cm}}$

Problem 4.3 (4) (1 point)

Compute these greatest common divisors with the Euclidean Algorithm:

$$\gcd(12, 34) = \underline{\hspace{2cm}}$$

$$\gcd(28, 25) = \underline{\hspace{2cm}}$$

$$\gcd(126, 216) = \underline{\hspace{2cm}}$$

$$\gcd(119, 196) = \underline{\hspace{2cm}}$$

$$\gcd(80, 100) = \underline{\hspace{2cm}}$$

$$\gcd(264, 407) = \underline{\hspace{2cm}}$$

Problem 4.3 (5) (1 point)

Compute these greatest common divisors with the Euclidean Algorithm:

$$\gcd(23, 25) = \underline{\hspace{2cm}}$$

$$\gcd(78, 93) = \underline{\hspace{2cm}}$$

$$\gcd(275, 385) = \underline{\hspace{2cm}}$$

$$\gcd(84, 189) = \underline{\hspace{2cm}}$$

$$\gcd(319, 352) = \underline{\hspace{2cm}}$$

$$\gcd(105, 238) = \underline{\hspace{2cm}}$$

Problem 4.3 (6) (1 point)

For each of the following pairs of numbers, find the greatest common divisor.

$$\gcd(30, 78) = \underline{\hspace{2cm}}$$

$$\gcd(189189, 189190) = \underline{\hspace{2cm}}$$

$$\gcd(65, 85) = \underline{\hspace{2cm}}$$

$$\gcd(798879, 1) = \underline{\hspace{2cm}}$$

$$\gcd(810277, 0) = \underline{\hspace{2cm}}$$

$\text{gcd}(10932, 10932) = \underline{\hspace{2cm}}$

Problem 4.3 (7) (1 point)

Consider the algorithm:

Algorithm

Input: A natural number v and a natural number k with $v > k$.

- (1) **repeat**
- (a) **let** $r := v \bmod k$
- (b) **let** $v := k$
- (c) **let** $k := r$
- (4) **until** $r = 0$
- (5) **return** v

What does the algorithm return when the input is $v := 39$ and $k := 24$? $\underline{\hspace{2cm}}$

What does the algorithm return when the input is $v := 128$ and $k := 24$? $\underline{\hspace{2cm}}$

What does the algorithm return when the input is $v := 87$ and $k := 24$? $\underline{\hspace{2cm}}$

What does the algorithm return when the input is $v := 30$ and $k := 24$? $\underline{\hspace{2cm}}$

What does the algorithm return ?

- A. $-v + k$
- B. k
- C. The quotient of the division of v by k .
- D. The remainder of the division of v by k .
- E. $k \cdot v$
- F. The greatest common divisor of k and v
- G. $(k)^v$
- H. The difference of the sum of the first v natural numbers and k .

Solutions

Problem 4.3 (1) *Correct Answers:*

- 4
- 24
- 4
- 0
- 4
- 0
- 4

Problem 4.3 (2) *Correct Answers:*

- 20
- 21
- 20
- 1
- 20
- 1
- 0
- 1
- 0
- 1

Problem 4.3 (3) *Correct Answers:*

Solution:

Sometimes it is easy to see the greatest common factor of two numbers. If you are trying a problem that does not look easy, it is often helpful to just do it one piece at a time.

Suppose you wanted to find $\gcd(120, 168)$. Well you can see that 2 divides both so put a 2 on your greatest common divisor list and divide the two numbers by 2 to see that you are now looking for $\gcd(60, 84)$. You might now notice either 2 or 4 is a factor of both. Suppose you noticed 4, Put it on your gcd list and divide to see that now you want $\gcd(15, 21)$. Now you see 3, which you can put on your gcd list and look for $\gcd(5, 7)$. But that is 1. So you can multiply the numbers on your gcd list to get $2 \times 4 \times 3 = 24$ and so 24 is your gcd.

In other cases, there is a method known as the Euclidean Algorithm which can compute greatest common divisor without factoring.

Correct Answers:

- 6
- 15
- 72

Problem 4.3 (4) *Correct Answers:*

- 2
- 1
- 18
- 7
- 20
- 11

Problem 4.3 (5) *Correct Answers:*

- 1
- 3
- 55
- 21
- 11
- 7

Problem 4.3 (6) *Correct Answers:*

Hint: Let a and b be an integers. Then

$$\gcd(a, b) = \gcd(b, a)$$

$$\gcd(a, a) = a$$

$$\gcd(a + 1, a) = 1$$

$$\gcd(1, a) = 1$$

$$\gcd(a, 0) = a$$

Correct Answers:

- 6
- 1
- 5
- 1
- 810277
- 10932

Problem 4.3 (7) *Correct Answers:*

- 3
- 8
- 3
- 6
- F

4.4 Bezouts-Identity

Problem 4.4 (1) (1 point)

Complete the statement of **Bezouts Identity** . We write $*$ for multiplication and $^{\wedge}$ for exponentiation.

Let f and h be natural numbers. Then there exist integers c and d such that

[select: | $(f * h)$ | $(c * f)$ | $(f + h)^2$ | $(c - f)^2$ | $(h - f)$ | $(c + f)$ | $(c * d)$ | $(c - f)$ | $(c * d)$ | $(f \bmod h)$]

+

[select: | $(f * h)$ | $(d + h)^2$ | $(f \operatorname{div} h)$ | $(d + h)$ | $(f + h)^2$ | $(h - f)$ | $(d * h)$ | $(c * d)$ | $(d - h)$ | $(d + c)$]

=

[select: | $(f \operatorname{div} h)$ | $(f \bmod h)$ | $\gcd(f, h)$ | $\gcd(c, h)$ | $\gcd(d, f)$ | $(d * h)$ | $(f + h)^2$ | $(c * d)$ | $(d + c)$ | (f^h)]

Problem 4.4 (2) (1 point)

Follow these step to compute the greatest common divisor of $a := 147$ and $b := 70$ and the integers s and t such that $(s \cdot a) + (t \cdot b) = \gcd(a, b)$.

First we compute $\gcd(a, b)$. In addition to the remainder we also compute the quotient.

Let $a_1 := b = \underline{\hspace{1cm}}$ and let $b_1 := a \bmod b = \underline{\hspace{1cm}}$ and let $q_1 := a \operatorname{div} b = \underline{\hspace{1cm}}$

Let $a_2 := b_1 = \underline{\hspace{1cm}}$ and let $b_2 := a_1 \bmod b_1 = \underline{\hspace{1cm}}$

We have computed $\gcd(147, 70) = b_1 = \underline{\hspace{1cm}}$.

Now write $a = (b \cdot q_1) + b_1$:

$\underline{\hspace{1cm}} = \left(\underline{\hspace{1cm}} \cdot \underline{\hspace{1cm}} \right) + \underline{\hspace{1cm}}$

Rearranging the values, write $b_1 = (1 \cdot a) + ((-q_1) \cdot b)$:

$\underline{\hspace{1cm}} = \left(1 \cdot \underline{\hspace{1cm}} \right) + \left(\underline{\hspace{1cm}} \cdot \underline{\hspace{1cm}} \right)$

Read off the values of s and t . Recall that $b_1 = \gcd(a, b)$.

With $s = \underline{\hspace{1cm}}$ and $t = \underline{\hspace{1cm}}$ we have $\gcd(a, b) = (s \cdot a) + (t \cdot b)$.

Problem 4.4 (3) (1 point)

Follow these step to compute the greatest common divisor of $a := 160$ and $b := 30$ and the integers s and t such that $(s \cdot a) + (t \cdot b) = \gcd(a, b)$.

First we compute $\gcd(a, b)$. In addition to the remainder we also compute the quotient.

Let $a_1 := b = \underline{\hspace{1cm}}$ and let $b_1 := a \bmod b = \underline{\hspace{1cm}}$ and let $q_1 := a \operatorname{div} b = \underline{\hspace{1cm}}$

Let $a_2 := b_1 = \underline{\hspace{1cm}}$ and let $b_2 := a_1 \bmod b_1 = \underline{\hspace{1cm}}$

We have computed $\gcd(160, 30) = b_1 = \underline{\hspace{1cm}}$.

Now write $a = (b \cdot q_1) + b_1$:

$$\underline{\hspace{1cm}} = \left(\underline{\hspace{1cm}} \cdot \underline{\hspace{1cm}} \right) + \underline{\hspace{1cm}}$$

Rearranging the values, write $b_1 = (1 \cdot a) + ((-q_1) \cdot b)$:

$$\underline{\hspace{1cm}} = \left(1 \cdot \underline{\hspace{1cm}} \right) + \left(\underline{\hspace{1cm}} \cdot \underline{\hspace{1cm}} \right)$$

Read off the values of s and t . Recall that $b_1 = \gcd(a, b)$.

With $s = \underline{\hspace{1cm}}$ and $t = \underline{\hspace{1cm}}$ we have $\gcd(a, b) = (s \cdot a) + (t \cdot b)$.

Problem 4.4 (4) (1 point)

Follow these step to compute the greatest common divisor of $a := 26$ and $b := 6$ and the integers s and t such that $(s \cdot a) + (t \cdot b) = \gcd(a, b)$.

First we compute $\gcd(a, b)$. In addition to the remainder we also compute the quotient.

Let $a_1 := b = \underline{\hspace{1cm}}$ and let $b_1 := a \bmod b = \underline{\hspace{1cm}}$ and let $q_1 := a \operatorname{div} b = \underline{\hspace{1cm}}$

Let $a_2 := b_1 = \underline{\hspace{1cm}}$ and let $b_2 := a_1 \bmod b_1 = \underline{\hspace{1cm}}$

We have computed $\gcd(26, 6) = b_1 = \underline{\hspace{1cm}}$.

Now write $a = (b \cdot q_1) + b_1$:

$$___ = \left(___ \cdot ___ \right) + ___$$

Rearranging the values, write $b_1 = (1 \cdot a) + ((-q_1) \cdot b)$:

$$___ = \left(1 \cdot ___ \right) + \left(___ \cdot ___ \right)$$

Read off the values of s and t . Recall that $b_1 = \gcd(a, b)$.

With $s = ___$ and $t = ___$ we have $\gcd(a, b) = (s \cdot a) + (t \cdot b)$.

Problem 4.4 (5) (1 point)

Compute the greatest common divisor of $a := 33$ and $b := 15$ and the integers s and t such that $(s \cdot a) + (t \cdot b) = \gcd(a, b)$.

We have $\gcd(33, 15) = ___$. Now find the numbers s and t whose existence is guaranteed by Bezout's identity.

With $s = ___$ and $t = ___$ we have $(s \cdot a) + (t \cdot b) = \gcd(a, b)$.

Problem 4.4 (6) (1 point)

Compute the greatest common divisor of $a := 36$ and $b := 7$ and the integers s and t such that $(s \cdot a) + (t \cdot b) = \gcd(a, b)$.

We have $\gcd(36, 7) = ___$. Now find the numbers s and t whose existence is guaranteed by Bezout's identity.

With $s = ___$ and $t = ___$ we have $(s \cdot a) + (t \cdot b) = \gcd(a, b)$.

Solutions

Problem 4.4 (1) *Correct Answers:*

- $(c * f)$
- $(d * h)$
- $\gcd(f, h)$

Problem 4.4 (2) *Correct Answers:*

- 70
- 7
- 2
- 7
- 0
- 7
- 147
- 70
- 2
- 7
- 7
- 147
- -2
- 70
- 1
- -2

Problem 4.4 (3) *Correct Answers:*

- 30
- 10
- 5
- 10
- 0
- 10
- 160
- 30
- 5
- 10
- 10
- 160
- -5
- 30
- 1
- -5

Problem 4.4 (4) *Correct Answers:*

- 6
- 2

- 4
- 2
- 0
- 2
- 26
- 6
- 4
- 2
- 2
- 26
- -4
- 6
- 1
- -4

Problem 4.4 (5) *Correct Answers:*

- 3
- 1
- -2

Problem 4.4 (6) *Correct Answers:*

- 1
- 1
- -5

Chapter 5

Sets

1. Sets
2. Roster Form
3. Membership and Equality
4. Special Sets
5. Set Builder Notation

5.1 Sets

Problem 5.1 (1) (1 point)

Complete the definitions:

A set is a well-defined (A) of distinct (B).

(A): [select: | **flock** | **pile** | **bucket** | **heap** | **collection** | **stack** | **pack** | **list**]

(B): [select: | **birds** | **bears** | **numbers** | **letters** | **words** | **objects**]

The (C) in a set are called (D) of the set.

(C): [select: | **birds** | **numbers** | **objects** | **letters** | **words** | **wolves**]

(D): [select: | **things** | **elements** | **animals** | **characters**]

Problem 5.1 (2) (1 point)

Determine which of the following are sets:

1. ___ The collection of students in all sections of MAT 112 this semester.
2. ___ The collection of beautiful houses.
3. ___ The collection of cuddly animals.
4. ___ The collection of difficult problems.

Problem 5.1 (3) (1 point)

Determine which of the following are sets:

1. ___ The collection of cuddly animals.
2. ___ The collection of integers.
3. ___ The collection of companies enjoying sizable profits.
4. ___ The collection of nice days.

Problem 5.1 (4) (1 point)

Find the quotient and remainder of the division of 36 by 9.

The quotient is ____

The remainder is ____

Let q be the quotient and let r the remainder. Enter thses values in the correct box below.

We have $36 = q \cdot 9 + r = ___ \cdot 9 + ___$.

Solutions

Problem 5.1 (1) *Correct Answers:*

- collection
 - objects
 - objects
 - elements
-

Problem 5.1 (2) *Correct Answers:*

- T
 - F
 - F
 - F
-

Problem 5.1 (3) *Correct Answers:*

- F
 - T
 - F
 - F
-

Problem 5.1 (4) *Correct Answers:*

- 4
- 0
- 4
- 0

5.2 Roster Form

Problem 5.2 (1) (1 point)

Complete the definition:

The contents of a set can be described by listing the elements of the set, separated by ^(A) between ^(B) .

(A): [select: | **commas** | **semicolons** | **colons** | **spaces**]

(B): [select: | **parenthesis** | **angle brackets** | **square brackets** | **curly brackets**]

This way of describing a set is called ^(C) .

(C): [select: | **rooster form** | **roster form** | **chicken form** | **list form** | **brace form** | **list**]

Problem 5.2 (2) (1 point)

Give the set of integers from 8 to 13 in roster form: {_____}

Problem 5.2 (3) (1 point)

Give the empty set in roster form: {_____}

Problem 5.2 (4) (1 point)

Give the set of natural numbers less than 2 in roster form: {_____}

Problem 5.2 (5) (1 point)

Give the set of natural numbers up to 1 in roster form: {_____}

Problem 5.2 (6) (1 point)

Give the set of negative integers greater than or equal to -9 in roster form: {_____}

Problem 5.2 (7) (1 point)

Give the set in roster form (without ellipsis): $\{5, 6, 7, \dots, 14\} = \{_____ \}$

Problem 5.2 (8) (1 point)

We have:

$$32 = 10 \cdot 3 + 2$$

Find the quotient and remainder of the division of 32 by 3.

The quotient is ____.

The remainder is ____.

Solutions

Problem 5.2 (1) *Correct Answers:*

- commas
 - curly brackets
 - roster form
-

Problem 5.2 (2) *Correct Answers:*

- 8, 9, 10, 11, 12, 13
-

Problem 5.2 (3) *Correct Answers:*

-
-

Problem 5.2 (4) *Correct Answers:*

- 1
-

Problem 5.2 (5) *Correct Answers:*

- 1
-

Problem 5.2 (6) *Correct Answers:*

- $-9, -8, -7, -6, -5, -4, -3, -2, -1$
-

Problem 5.2 (7) *Correct Answers:*

- 5, 6, 7, 8, 9, 10, 11, 12, 13, 14
-

Problem 5.2 (8) *Correct Answers:*

- 10
- 2

5.3 Membership and Equality

Problem 5.3 (1) (1 point)

Complete the following:

Let A and B be sets.

When b ^(A) the set A we write $b \in A$.

(A): [select: | **is related to** | **is an element of** | **is equal to** | **is not related to** | **is not an element of** | **is not equal to**]

When b ^(B) the set A we write $b \notin A$.

(B): [select: | **is related to** | **is an element of** | **is equal to** | **is not related to** | **is not an element of** | **is not equal to**]

We say the set A ^(C) the set B and write $A = B$ if each element in the set A ^(D) the set B and if each element in the set B ^(E) the set A .

(C): [select: | **is related to** | **is an element of** | **is equal to** | **is not related to** | **is not an element of** | **is not equal to**]

(D): [select: | **is related to** | **is an element of** | **is equal to** | **is not related to** | **is not an element of** | **is not equal to**]

(E): [select: | **is related to** | **is an element of** | **is equal to** | **is not related to** | **is not an element of** | **is not equal to**]

If the set A ^(F) the set B we write $A \neq B$.

(F): [select: | **is related to** | **is an element of** | **is equal to** | **is not related to** | **is not an element of** | **is not equal to**]

Problem 5.3 (2) (1 point)

Let $C = \{0, 3, 5, 6\}$.

For each statement indicate whether it is true or false.

1. ☐ $\{0, 5, 6\} = C$
2. ☐ $\{\} \neq C$
3. ☐ $C = \{6\}$
4. ☐ $C = \{5, 3, 0\}$

Problem 5.3 (3) (1 point)

Let $B = \{5, 9, 11, 14, 18, 19, 20\}$.

For each statement indicate whether it is true or false.

1. ☐ $B = \{9, 11, 14, 19, 20, 5\}$
2. ☐ $B = \{5, 9, 11, 14, 18, 19, 20\}$
3. ☐ $B \neq \{11, 14, 9, 19, 18, 20, 5\}$
4. ☐ $B = \{5, 16, 11, 14, 18, 19, 20\}$

Problem 5.3 (4) (1 point)

For the given sets C and D determine whether the statement

$$C = D$$

is true or false. If the statement is false choose the reason.

1. ☐ when $C := \{4, 1, 0, 2\}$ and $D := \{2, 1, 0\}$
2. ☐ when $C := \{4, 1, 0, 2\}$ and $D := \{2, 1, 0, 4\}$
3. ☐ when $C := \{0, 1, 2\}$ and $D := \{2, 1, 0\}$
4. ☐ when $C := \{5, 4\}$ and $D := \{4, 5\}$

Problem 5.3 (5) (1 point)

Let $S = \{7, 8, 9, \dots, 37\}$. For each statement indicate whether it is true or false.

1. ☐ $5 \notin S$
2. ☐ $40 \in S$

3. ☐ $13 \in S$

4. ☐ $-3 \in S$

Problem 5.3 (6) (1 point)

Let $A = \{11, 16, 19, 24, 27, 30, 32, 37, 41, 46\}$. For each statement indicate whether it is true or false.

1. ☐ $23 \notin A$

2. ☐ $27 \in \{\}$

3. ☐ $20 \in A$

4. ☐ $2 \in A$

Problem 5.3 (7) (1 point)

Let $A = \{43, 44, 45, \dots, 50\}$.

Is the statement $57 \in A$ true or false ?

- A. True
- B. False

Is the statement $58 \in A$ true or false ?

- A. False
- B. True

Is the statement $39 \in A$ true or false ?

- A. True
- B. False

Problem 5.3 (8) (1 point)

Let $S = \{-1, 1, \{3\}, 7, \{11, 14\}, 14\}$.

For each statement indicate whether it is true or false.

1. ☐ $1 \in S$

2. ☐ $-6 \in S$

3. ☐ $14 \in S$

4. $3 \notin S$

Problem 5.3 (9) (1 point)

Let $A = \{7, 8, 9, \dots, 11\}$ and $b = 15$.

Is $b \notin A$ true or false ?

- A. False
- B. True

Problem 5.3 (10) (1 point)

We have:

$$74781944687 = 131785 \cdot 567452 + 282867$$

Find the quotient and remainder of the division of 74781944687 by 567452.

The quotient is _____.

The remainder is _____.

Solutions

Problem 5.3 (1) *Correct Answers:*

- is an element of
 - is not an element of
 - is equal to
 - is an element of
 - is an element of
 - is not equal to
-

Problem 5.3 (2) *Correct Answers:*

- F
 - T
 - F
 - F
-

Problem 5.3 (3) *Correct Answers:*

- F
 - T
 - F
 - F
-

Problem 5.3 (4) *Correct Answers:*

- 4 not in D
 - True
 - True
 - True
-

Problem 5.3 (5) *Correct Answers:*

- T
 - F
 - T
 - F
-

Problem 5.3 (6) *Correct Answers:*

- T
- F
- F
- F

Problem 5.3 (7) *Correct Answers:*

- B
- A
- B

Problem 5.3 (8) *Correct Answers:*

- T
- F
- T
- T

Problem 5.3 (9) *Correct Answers:*

- B

Problem 5.3 (10) *Correct Answers:*

Hint: Let a be an integer and b a natural number.

Suppose $a = b \cdot q + r$ with $0 \leq r < b$. Then the quotient is $q = a \operatorname{div} b$ and the remainder is $r = a \bmod b$.

In this problem $a = 74781944687$ and $b = 567452$.

Correct Answers:

- 131785
- 282867

5.4 Special Sets

Problem 5.4 (1) (1 point)

Special Sets

Match the two representation of sets. Enter the letters next to the numbers.

- | | |
|--------------------------|---|
| ___ 1. $\{\}$ | A. $\{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ |
| ___ 2. $\mathbb{Z}_{16}$ | B. the set that contains no elements |
| ___ 3. $\mathbb{Z}$ | C. $\{0, 1, 2, 3, \dots, 15\}$ |
-

Problem 5.4 (2) (1 point)

Special Sets

Match the two representation of sets. Enter the letters next to the numbers.

- | | |
|---|--------------------------------|
| ___ 1. 'Z 22' | A. $\mathbb{Z}_{12}$ |
| ___ 2. the set of integers from 0 to 11 | B. $\mathbb{Z}_{22}$ |
| ___ 3. 'Z 22 without zero' | C. $\mathbb{Z}_{22}^{\otimes}$ |
-

Problem 5.4 (3) (1 point)

For each statement indicate whether it is true or false.

1. ___ $\{0\} \neq \{\}$
 2. ___ $\{\} = \{0\}$
 3. ___ $0 \notin \{\}$
 4. ___ $\{\} = \mathbb{Z}$
-

Problem 5.4 (4) (1 point)

Give the set in roster form. $\mathbb{Z}_6 = \{\text{_____}\}$

Problem 5.4 (5) (1 point)

Give the set in roster form. $\mathbb{Z}_4^\otimes = \{\text{_____}\}$

Problem 5.4 (6) (1 point)

For each statement indicate whether it is true or false.

1. ☐ $r \in \mathbb{A}$
2. ☐ $h \in \mathbb{A}$
3. ☐ $5 \notin \mathbb{A}$
4. ☐ $41 \in \{\}$
5. ☐ $a \in \mathbb{A}$

Problem 5.4 (7) (1 point)

For each statement indicate whether it is true or false.

1. ☐ $8 \notin \mathbb{A}$
2. ☐ $\{\} = \mathbb{Z}$
3. ☐ $z \notin \mathbb{A}$
4. ☐ $0 \in \mathbb{Z}_8^\otimes$

Problem 5.4 (8) (1 point)

For each statement indicate whether it is true or false.

1. ☐ $6 \notin \mathbb{A}$
2. ☐ $65 \notin \mathbb{Z}_{63}$
3. ☐ $0 \in \mathbb{Z}_6$
4. ☐ $6 \in \mathbb{A}$

Problem 5.4 (9) (1 point)

Decide which of the following are true statements, or false statements. If in doubt try out the statement with the ‘for all’ variables replaced by some numbers.

1. ☐ For all $a \in \mathbb{Z}$ and for all $b \in \mathbb{Z}$ we have $(a \cdot b)^2 = a^2 + b^2$.
2. ☐ For all $a \in \mathbb{Z}$ we have $a \cdot 0 = a$.

3. ____ For all $a \in \mathbb{Z}$ we have $a + 0 = a$.

4. ____ For all $a \in \mathbb{Z}$ and for all $b \in \mathbb{Z}$ and for all $n \in \mathbb{N}$ we have $(a \cdot b)^n = (a^n) \cdot (b^n)$.

Problem 5.4 (10) (1 point)

Compute these remainders:

$$1 \bmod 7 = \underline{\hspace{1cm}}$$

$$179 \bmod 4 = \underline{\hspace{1cm}}$$

$$176 \bmod 9 = \underline{\hspace{1cm}}$$

$$179 \bmod 13 = \underline{\hspace{1cm}}$$

$$169 \bmod 15 = \underline{\hspace{1cm}}$$

$$189 \bmod 11 = \underline{\hspace{1cm}}$$

Solutions

Problem 5.4 (1) *Correct Answers:*

- B
- C
- A

Problem 5.4 (2) *Correct Answers:*

- B
- A
- C

Problem 5.4 (3) *Correct Answers:*

- T
- F
- T
- F

Problem 5.4 (4) *Correct Answers:*

- 0, 1, 2, 3, 4, 5

Problem 5.4 (5) *Correct Answers:*

- 1, 2, 3

Problem 5.4 (6) *Correct Answers:*

- T
- T
- T
- F
- T

Problem 5.4 (7) *Correct Answers:*

Hint: $\mathbb{A} = \{-, a, b, c, \dots, z\}$

$\mathbb{Z}_n = \{0, 1, 2, 3, \dots, n-1\}$

$\mathbb{Z}_n^\otimes = \{1, 2, 3, \dots, n-1\}$

Correct Answers:

- T
- F
- F
- F

Problem 5.4 (8) *Correct Answers:*

Hint: $\mathbb{A} = \{-, a, b, c, \dots, z\}$

$\mathbb{Z}_n = \{0, 1, 2, 3, \dots, n-1\}$

$\mathbb{Z}_n^\otimes = \{1, 2, 3, \dots, n-1\}$

Correct Answers:

- T
- T
- T
- F

Problem 5.4 (9) *Correct Answers:*

- F
- F
- T
- T

Problem 5.4 (10) *Correct Answers:*

- 1
- 3
- 5
- 10
- 4
- 2

5.5 Set Builder Notation

Problem 5.5 (1) (1 point)

Consider:

$$\{a \mid a \in \mathbb{Z} \text{ and } a \geq -6 \text{ and } a \leq -2\}$$

This is read as:

The set (A) a (B) a is (C) the set of (D) and a is (E) -6 and a is (F) -2 .

(A): [select: | **of the one element** | **of all elements**]

(B): [select: | **where** | **with the exception that**]

(C): [select: | **an element of** | **not an element of** | **less than** | **greater than** | **equal to**]

(D): [select: | **natural numbers** | **integers** | **negative integers** | **characters**]

(E): [select: | **less than** | **less than or equal to** | **greater than** | **greater than or equal to** | **equal to** | **not equal to** | **better than** | **worse than**]

(F): [select: | **less than** | **less than or equal to** | **greater than** | **greater than or equal to** | **equal to** | **not equal to** | **better than** | **worse than**]

Give the set in roster form. {_____}

Problem 5.5 (2) (1 point)

Give the set in roster form.

$$\{x \mid x \in \mathbb{Z} \text{ and } x > -3 \text{ and } x \leq 3\} = \{ \text{_____} \}$$

Problem 5.5 (3) (1 point)

Give the set in roster form (without ellipsis).

$$\{x \mid x \in \mathbb{N} \text{ and } x \geq 27 \text{ and } x \leq 50 \text{ and } x \bmod 9 = 0\} = \{ \text{_____} \}$$

Problem 5.5 (4) (1 point)

Give the set in roster form.

$$\{x \mid x \in \mathbb{N} \text{ and } x < 17\} = \{\rule{1.5cm}{0.4pt}\}$$

Problem 5.5 (5) (1 point)

Give the set in roster form.

$$\{x \mid x \in \mathbb{N} \text{ and } x \leq 16 \text{ and } x \bmod 14 = 0\} = \{\rule{1.5cm}{0.4pt}\}$$

[although it is mathematically correct to list elements multiple times, this problem is marked wrong if you do so.]

Problem 5.5 (6) (1 point)

Let $S = \{0, 1, 2, 3, 4, 5\}$.

For each statement indicate whether it is true or false.

1. ☐ $S = \{5, 4, 3, 2, 1, 0\}$
 2. ☐ $S = \{x \mid x \in \mathbb{N} \text{ and } x \leq 5\}$
 3. ☐ $S = \{1, 2, 3, 4, 5\}$
 4. ☐ $S = \{x \mid x \text{ is an integer from 0 to 5}\}$
-

Problem 5.5 (7) (1 point)

Compute

$$(2 + 0^3) \bmod 5 = \rule{1cm}{0.4pt}$$

$$(2 + 1^3) \bmod 5 = \rule{1cm}{0.4pt}$$

$$(2 + 2^3) \bmod 5 = \rule{1cm}{0.4pt}$$

$$(2 + 3^3) \bmod 5 = \rule{1cm}{0.4pt}$$

$$(2 + 4^3) \bmod 5 = \rule{1cm}{0.4pt}$$

Now find $\{(x, (2 + x^3) \bmod 5) \mid x \in \mathbb{Z}_5\} = \{\rule{1.5cm}{0.4pt}\} \subseteq \mathbb{Z}_5 \times \mathbb{Z}_5$.

Problem 5.5 (8) (1 point)

Give the set in roster form.

$$\{x + 18 \mid x \in \mathbb{Z} \text{ and } x \geq -7 \text{ and } x < 3\} = \{ \rule{1.5cm}{0.4pt} \}$$

Solutions

Problem 5.5 (1) *Correct Answers:*

- of all elements
 - where
 - an element of
 - integers
 - greater than or equal to
 - less than or equal to
 - $\{-6, -5, -4, -3, -2\}$
-

Problem 5.5 (2) *Correct Answers:*

- $\{-2, -1, 0, 1, 2, 3\}$
-

Problem 5.5 (3) *Correct Answers:*

- $\{27, 36, 45\}$
-

Problem 5.5 (4) *Correct Answers:*

- $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}$
-

Problem 5.5 (5) *Correct Answers:*

- 14
-

Problem 5.5 (6) *Correct Answers:*

- T
 - F
 - F
 - T
-

Problem 5.5 (7) *Correct Answers:*

Correct Answers:

- 2
 - 3
 - 0
 - 4
 - 1
 - $\{(3, 4), (1, 3), (0, 2), (4, 1), (2, 0)\}$
-

Problem 5.5 (7) *Correct Answers:*

- $\{11, 12, 13, 14, 15, 16, 17, 18, 19, 20\}$

Chapter 6

More on Sets

1. Subsets
2. Cartesian Products
3. Applications of Cartesian Products

6.1 Subsets

Problem 6.1 (1) (1 point)

Complete the following:

Let A and B be sets.

We say the set A is $\underline{\quad (A) \quad}$ of the set B and write $A \subseteq B$ if $\underline{\quad (B) \quad}$ of A $\underline{\quad (C) \quad}$ the set B .

(A): [select: | **a superset** | **a subset** | **an under set** | **not a superset** | **not a subset** | **not an under set**]

(B): [select: | **each element** | **there is an element** | **no element**]

(C): [select: | **is related to** | **is an element of** | **is equal to** | **is not related to** | **is not an element of** | **is not equal to**]

We say the set A is $\underline{\quad (D) \quad}$ of the set B and write $A \not\subseteq B$ if $\underline{\quad (E) \quad}$ of A that $\underline{\quad (F) \quad}$ the set B .

(A): [select: | **a superset** | **a subset** | **an under set** | **not a superset** | **not a subset** | **not an under set**]

(B): [select: | **each element** | **no element** | **there is an element** | **there are two element**]

(C): [select: | **is related to** | **is an element of** | **is equal to** | **is not related to** | **is not an element of** | **is not equal to**]

Problem 6.1 (2) (1 point)

For each statement indicate whether it is true or false.

1. $\underline{\quad} \{\} \in \{-2, 3, 7\}$

2. $\underline{\quad} \{\} \subseteq \{-2, 3, 7\}$

3. $\underline{\quad} \{\} \subseteq \{0\}$

4. $\underline{\quad} \{\} \in \{\}$

Problem 6.1 (3) (1 point)

For the given sets C and D determine whether the statement

$$C \subseteq D$$

is true or false. If the statement is false choose the reason.

___ when $C := \{5\}$ and $D := \{\}$

1. ___ when $C := \{4, 1, 0, 2\}$ and $D := \{2, 1, 0\}$

2. ___ when $C := \{4, 1, 0, 2\}$ and $D := \{2, 4, 1, 0, 5\}$

3. ___ when $C := \{5\}$ and $D := \{4, 5\}$

Problem 6.1 (4) (1 point)

For the given sets C and D determine whether the statement

$$C \subseteq D$$

is true or false. If the statement is false choose the reason.

1. ___ when $C := \{14\}$ and $D := \{13, 14\}$

2. ___ when $C := \{10, 11, 12\}$ and $D := \{9, 10, 11, 12\}$

3. ___ when $C := \{9, 10, 11\}$ and $D := \{9, 10, 11, 12\}$

4. ___ when $C := \{13, 10, 9, 11\}$ and $D := \{11, 13, 10, 9, 14\}$

Problem 6.1 (5) (1 point)

For each statement indicate whether it is true or false.

1. ___ $\{\} \in \{0, 6, 9\}$

2. ___ $\{\} \subseteq \{0, 6, 9\}$

3. ___ $0 \in \{\}$

4. ___ $0 \in \{0\}$

Problem 6.1 (6) (1 point)

Let $A = \{16, 4, 6\}$, $B = \{16, 6\}$, $C = \{4, 6\}$, and $D = \{4, 6, 29\}$.

For each statement indicate whether it is true or false.

1. ___ $B \not\subseteq D$

2. $\text{--- } C \subseteq D$

3. $\text{--- } B \not\subseteq A$

4. $\text{--- } A \subseteq B$

Problem 6.1 (7) (1 point)

For each statement indicate whether it is true or false.

1. $\text{--- } \{0, 1, 2, \dots, 7\} \subseteq \mathbb{Z}_{23}^{\otimes}$

2. $\text{--- } \mathbb{Z}_{23} \subseteq \{0, 1, 2, \dots, 23\}$

3. $\text{--- } \mathbb{Z}_{19} \subseteq \{\}$

4. $\text{--- } \{0\} \subseteq \{\}$

Problem 6.1 (8) (1 point)

Let $E = \{a, b, c, f, g\}$.

For each statement indicate whether it is true or false.

1. $\text{--- } \{b, c, f\} \subseteq E$

2. $\text{--- } \{a, b, c, f, g\} \subseteq E$

3. $\text{--- } \{c\} \subseteq E$

4. $\text{--- } \{f, g\} \not\subseteq E$

Problem 6.1 (9) (1 point)

For each statement indicate whether it is true or false.

1. $\text{--- } \{\} \subseteq \{\{\}\}$

2. $\text{--- } \{\} \not\subseteq \{3, 8, 17, 23\}$

3. $\text{--- } \{\} \not\subseteq \{\}$

4. $\text{--- } \{\{\}\} \subseteq \{\{\}, \{\{\}\}, 0, 1\}$

Problem 6.1 (10) (1 point)

Let A and B be sets. For each statement indicate whether it is true or false.

1. ____ If there is $a \in A$ such that $a \notin B$ then $A = B$.
2. ____ If there is $a \in A$ such that $a \notin B$ then $A \subseteq B$.
3. ____ If $A \subseteq B$ and $B \not\subseteq A$ then $A = B$.
4. ____ If $A \subseteq B$ and $B \subseteq A$ then $A = B$.

Problem 6.1 (11) (1 point)

Let $A = \{2, 4, 6\}$, $B = \{2, 6\}$, $C = \{4, 6\}$ and $D = \{4, 6, 8\}$. Determine which of these sets are subsets of which other of these sets.

Check ALL true statements.

- A. $C \subseteq A$
- B. $A \subseteq C$
- C. $\{\} \subseteq D$
- D. $D \subseteq C$
- E. $B \subseteq C$
- F. $B \subseteq A$
- G. $A \subseteq B$
- H. $C \subseteq D$

Problem 6.1 (12) (1 point)

Find the quotients and remainders:

$$9 \text{ div } 7 = \underline{\hspace{2cm}} \text{ and } 9 \text{ mod } 7 = \underline{\hspace{2cm}}$$

$$-48 \text{ div } 22 = \underline{\hspace{2cm}} \text{ and } -48 \text{ mod } 22 = \underline{\hspace{2cm}}$$

$$17 \text{ div } 14 = \underline{\hspace{2cm}} \text{ and } 17 \text{ mod } 14 = \underline{\hspace{2cm}}$$

$$-45 \text{ div } 28 = \underline{\hspace{2cm}} \text{ and } -45 \text{ mod } 28 = \underline{\hspace{2cm}}$$

Solutions

Problem 6.1 (1) *Correct Answers:*

- a subset
 - each element
 - is an element of
 - not a subset
 - there is an element
 - is not an element of
-

Problem 6.1 (2) *Correct Answers:*

Hint: We denote the empty set by $\{\}$. The empty set has no elements. However, because the definition of subset reads $S \subseteq T$ if and only if $x \in S$ then $x \in T$, the empty set is a subset of all sets.

Correct Answers:

- F
 - T
 - T
 - F
-

Problem 6.1 (3) *Correct Answers:*

- 5 not in D
 - 4 not in D
 - True
 - True
-

Problem 6.1 (4) *Correct Answers:*

- True
 - True
 - True
 - True
-

Problem 6.1 (5) *Correct Answers:*

Hint: The empty set has no elements. However, because the definition of subset reads $S \subseteq T$ if and only if $x \in S$ then $x \in T$, the empty set is a subset of all sets. The empty set is an element of a set T , only if T contains the empty set.

Correct Answers:

- F
 - T
 - F
 - T
-

Problem 6.1 (6) *Correct Answers:*

- T
- T
- F

- F

Problem 6.1 (7) *Correct Answers:*

Hint: $\mathbb{Z}_n = \{0, 1, 2, 3, \dots, n-1\}$

$\mathbb{Z}_n^\otimes = \{1, 2, 3, \dots, n-1\}$

Correct Answers:

- F
- T
- F
- F

Problem 6.1 (8) *Correct Answers:*

Solution:

$E = \{a, b, c, f, g\}$

Subsets of E include:

$\{a, f, g\}$

$\{a, b, c, f, g\}$

Remember that a set is always a subset of itself. By definition, for sets A and B , $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$. From this definition, it is clear that since $A = A$ for any set A , $A \subseteq A$ must also be true.

Correct Answers:

- T
- T
- T
- F

Problem 6.1 (9) *Correct Answers:*

- T
- F
- F
- T

Problem 6.1 (10) *Correct Answers:*

- F
- F
- F
- T

Problem 6.1 (11) *Correct Answers:*

- ACFH

Problem 6.1 (12) *Correct Answers:*

Correct Answers:

- 1
- 2
- -3
- 18
- 1
- 3
- -2
- 11

6.2 Cartesian Products

Problem 6.2 (1) (1 point)

Complete the following:

Let A and B be sets.

The ^(A) of the sets A and B , denoted by $A \times B$, is the set of all ^(B) (a, b) where a is ^(C) the set A
^(D) b is ^(E) the set B .

(A): [select: | **intersection** | **union** | **difference** | **sum** | **Cartesian product** | **complement**]

(B): [select: | **unordered pairs** | **ordered pairs** | **sets** | **numbers**]

(C): [select: | **related to** | **an element of** | **a subsets of** | **not related to** | **not an element of** | **a proper subset of** | **equal to** | **not equal to**]

(D): [select: | **and** | **or**]

(E): [select: | **related to** | **an element of** | **a subsets of** | **not related to** | **not an element of** | **a proper subset of** | **equal to** | **not equal to**]

Problem 6.2 (2) (1 point)

Let $A = \{7, 8, 9, \dots, 20\}$

Let $B = \{-6, -5, -4, \dots, 3\}$

Determine which of the following are in $A \times B$ (Check all that apply).

- A. $(10, -10)$
- B. $(24, 13)$
- C. $(11, 0)$
- D. $(4, 4)$
- E. $(9, 14)$
- F. $(16, -5)$
- G. $(14, -4)$
- H. $(12, 0)$
- I. $(18, -1)$
- J. $(4, -6)$

Problem 6.2 (3) (1 point)

Let $D = \{v, z, p\}$ and $H = \{d, z\}$.

Determine whether the following statements are true or false.

1. ☐ $(z, z) \in D \times H$

2. ☐ $(z, d) \in H \times H$

3. ☐ $(v, v) \in D \times D$

4. ☐ $(z, p) \in D \times H$

Problem 6.2 (4) (1 point)

Let $A = \{2, 3, 4\}$ and let $B = \{2, 3\}$. Give the set in roster form.

$A \times B = \{ \rule{1.5cm}{0.4pt} \}$

Problem 6.2 (5) (1 point)

Let $A = \{2, 3, 4, 5\}$. Give the set in roster form.

$\{(a, 9 \cdot a) \mid a \in A\} = \{ \rule{1.5cm}{0.4pt} \}$

[although it would be mathematically correct to list elements multiple times, this problem is marked wrong if you do so.]

Problem 6.2 (6) (1 point)

Let $A = \{-5, -4, -3, -2, -1\}$. Give the set in roster form.

$\{(a, a \bmod 4) \mid a \in A\} = \{ \rule{1.5cm}{0.4pt} \}$

[although it would be mathematically correct to list elements multiple times, this problem is marked wrong if you do so.]

Problem 6.2 (7) (1 point)

Let $A = \{10, 11, 12\}$ and let $B = \{1\}$. Give the set in roster form.

$A \times B = \{ \rule{1.5cm}{0.4pt} \}$

Problem 6.2 (8) (1 point)

Let a be an integer.

Suppose that the remainder when a is divided by 4 is 0 and the remainder when b is divided by 4 is 1.

That is, $a \bmod 4 = 0$ and $b \bmod 4 = 1$.

Find:

$$(a + a) \bmod 4 = \underline{\hspace{1cm}}$$

$$(a + b) \bmod 4 = \underline{\hspace{1cm}}$$

$$(a \cdot b) \bmod 4 = \underline{\hspace{1cm}}$$

$$(a + 2) \bmod 4 = \underline{\hspace{1cm}}$$

$$(2 \cdot b) \bmod 4 = \underline{\hspace{1cm}}$$

Solutions

Problem 6.2 (1) *Correct Answers:*

- Cartesian product
 - ordered pairs
 - an element of
 - and
 - an element of
-

Problem 6.2 (2) *Correct Answers:*

- CFGHI
-

Problem 6.2 (3) *Correct Answers:*

- T
 - T
 - T
 - F
-

Problem 6.2 (4) *Correct Answers:*

- $(2,2), (2,3), (3,2), (3,3), (4,2), (4,3)$
-

Problem 6.2 (5) *Correct Answers:*

- $(2,18), (3,27), (4,36), (5,45)$
-

Problem 6.2 (6) *Correct Answers:*

- $(-5,3), (-4,0), (-3,1), (-2,2), (-1,3)$
-

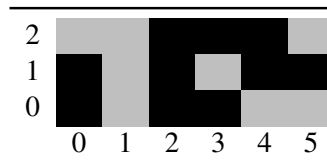
Problem 6.2 (7) *Correct Answers:*

- $(10,1), (11,1), (12,1)$
-

Problem 6.2 (8) *Correct Answers:*

- 0
- 1
- 0
- 2
- 2

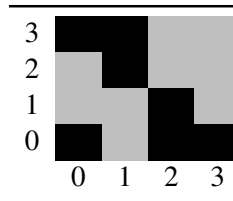
6.3 Applications of Cartesian Products

Problem 6.3 (1) (1 point)

The subset of $\{0, 1, 2, 3, 4, 5\} \times \{0, 1, 2\}$ represented by the black pixels in the raster above is:

{_____}

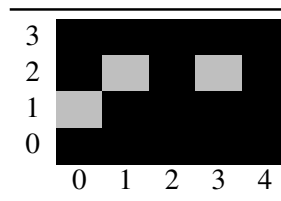
[although it would be mathematically correct, answers with repeated elements will be marked as wrong]

Problem 6.3 (2) (1 point)

The subset of $\{0, 1, 2, 3\} \times \{0, 1, 2, 3\}$ represented by the black pixels in the raster above is:

{_____}

[although it would be mathematically correct, answers with repeated elements will be marked as wrong]

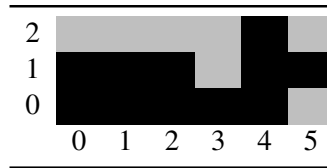
Problem 6.3 (3) (1 point)

The subset of $\{0, 1, 2, 3, 4\} \times \{0, 1, 2, 3\}$ represented by the black pixels in the raster above is:

{_____}

[although it would be mathematically correct, answers with repeated elements will be marked as wrong]

Problem 6.3 (4) (1 point)



The subset of $\{0, 1, 2, 3, 4, 5\} \times \{0, 1, 2\}$ represented by the black pixels in the raster above is:

{_____}

[although it would be mathematically correct, answers with repeated elements will be marked as wrong]

Problem 6.3 (5) (1 point)

Find the quotients and remainders:

$6 \text{ div } 2 = \underline{\hspace{1cm}}$ and

$6 \text{ mod } 2 = \underline{\hspace{1cm}}$

$-44 \text{ div } 21 = \underline{\hspace{1cm}}$ and

$-44 \text{ mod } 21 = \underline{\hspace{1cm}}$

$24 \text{ div } 11 = \underline{\hspace{1cm}}$ and

$24 \text{ mod } 11 = \underline{\hspace{1cm}}$

$-46 \text{ div } 27 = \underline{\hspace{1cm}}$ and

$-46 \text{ mod } 27 = \underline{\hspace{1cm}}$

Solutions

Problem 6.3 (1) *Correct Answers:*

- $(2, 2), (3, 2), (4, 2), (0, 1), (2, 1), (4, 1), (5, 1), (0, 0), (2, 0), (3, 0)$
-

Problem 6.3 (2) *Correct Answers:*

- $(0, 3), (1, 3), (1, 2), (2, 1), (0, 0), (2, 0), (3, 0)$
-

Problem 6.3 (3) *Correct Answers:*

- $(0, 3), (1, 3), (2, 3), (3, 3), (4, 3), (0, 2), (2, 2), (4, 2), (1, 1), (2, 1), (3, 1), (4, 1), (0, 0), (1, 0), (2, 0), (3, 0), (4, 0)$
-

Problem 6.3 (4) *Correct Answers:*

- $(4, 2), (0, 1), (1, 1), (2, 1), (4, 1), (5, 1), (0, 0), (1, 0), (2, 0), (3, 0), (4, 0)$
-

Problem 6.3 (5) *Correct Answers:*

Correct Answers:

- 3
- 0
- -3
- 19
- 2
- 2
- -2
- 8

Chapter 7

Functions

1. Definition of Function
2. Equality of Functions
3. Composite Functions
4. Identity Functions
5. Inverse Functions

7.1 Definition of Function

Problem 7.1 (1) (1 point)

Complete the following:

Let A and B be nonempty sets.

A function from A to B assigns ^(A) of B to ^(B) of A .

(A): [select: | **two elements** | **each element** | **no element** | **half of the elements** | **exactly one element** | **some element**]

(B): [select: | **two elements** | **each element** | **no element** | **half of the elements** | **exactly one element** | **some element**]

The set A is called the ^(C) of the function and the set B is called the ^(D) of the function.

(C): [select: | **range** | **image** | **subset** | **codomain** | **domain** | **superset** | **preimage** | **function**]

(D): [select: | **range** | **image** | **subset** | **codomain** | **domain** | **superset** | **preimage** | **function**]

Problem 7.1 (2) (1 point)

Let $g : \mathbb{Z}_{16} \rightarrow \mathbb{Z}_{20}$. Identify the following:

1. g
2. $\mathbb{Z}_{16}$
3. $g(11)$
4. $\mathbb{Z}_{20}$

Problem 7.1 (3) (1 point)

Let $f : \mathbb{Z} \rightarrow \mathbb{Z}_8$, $f(x) = (x) \bmod 8$. Find:

$f(3) = \underline{\hspace{1cm}}$

$f(-5) = \underline{\hspace{1cm}}$

$$f(16) = \underline{\hspace{2cm}}$$

Problem 7.1 (4) (1 point)

Let the function $k : \mathbb{Z}_9 \rightarrow \mathbb{Z}_7$ be given by $k(x) = (1 + x^3) \bmod 7$.

Find k evaluated at all elements of its domain.

$$k(0) = \underline{\hspace{2cm}}$$

$$k(1) = \underline{\hspace{2cm}}$$

$$k(2) = \underline{\hspace{2cm}}$$

$$k(3) = \underline{\hspace{2cm}}$$

$$k(4) = \underline{\hspace{2cm}}$$

$$k(5) = \underline{\hspace{2cm}}$$

$$k(6) = \underline{\hspace{2cm}}$$

$$k(7) = \underline{\hspace{2cm}}$$

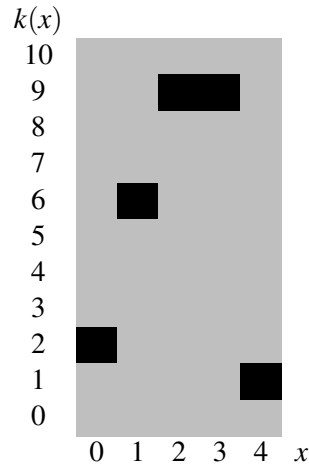
$$k(8) = \underline{\hspace{2cm}}$$

In roster form the image of A under k is $\{k(x) \mid x \in \mathbb{Z}_9\} = \{\underline{\hspace{2cm}}\}$.

In roster form the graph of k is $\{(x, k(x)) \mid x \in \mathbb{Z}_9\} = \{\underline{\hspace{2cm}}\}$.

Problem 7.1 (5) (1 point)

Suppose that the graph of the function k is given by



In roster form the graph of k is $\{ \rule{1.5cm}{0.4pt} \}$.

In roster form the domain of k is $A = \{ \rule{1.5cm}{0.4pt} \}$.

In roster form the codomain of k is $B = \{ \rule{1.5cm}{0.4pt} \}$.

Find k evaluated at all elements of its domain.

$$k(0) = \rule{1cm}{0.4pt}$$

$$k(1) = \rule{1cm}{0.4pt}$$

$$k(2) = \rule{1cm}{0.4pt}$$

$$k(3) = \rule{1cm}{0.4pt}$$

$$k(4) = \rule{1cm}{0.4pt}$$

In roster form the image of A under k is $\{k(x) \mid x \in A\} = \{ \rule{1.5cm}{0.4pt} \}$.

Problem 7.1 (7) (1 point)

Consider the function $G : \mathbb{Z} \rightarrow \mathbb{Z}$ defined by $G(x) = -2x^2 - 3x + 3$.

Evaluate the following:

a. $G(0) = \rule{1cm}{0.4pt}$

b. $G(-2) = \rule{1cm}{0.4pt}$

Problem 7.1 (8) (1 point)

Let $S := \{-10, -5, 0, 5, 10\}$ and let $g : S \rightarrow S$ be given by the following table of values.

y	-10	-5	0	5	10
$g(y)$	-10	0	5	-5	10

Use the table to fill in the missing values. There may be more than one correct answer, in which case you should enter your answers as a comma separated list. If there are no correct answers, enter *NONE*. help (numbers)

$$g(0) = \underline{\hspace{2cm}}$$

$$g(5) = \underline{\hspace{2cm}}$$

$$g(\underline{\hspace{2cm}}) = 0$$

$$g(\underline{\hspace{2cm}}) = 5$$

Problem 7.1 (9) (1 point)

Consider the function

$$g : \{-2, -1, \dots, 6, 7\} \rightarrow \{-2, -1, \dots, 6, 7\}$$

x	-2	-1	0	1	2	3	4	5	6	7
$g(x)$	6	0	4	5	2	-2	1	-1	3	6

Find $g(-2)$.

$$g(-2) = \underline{\hspace{2cm}}$$

Problem 7.1 (10) (1 point)

Let $f : \mathbb{Z}_3 \rightarrow \mathbb{Z}_3$, $f(x) = (0) \bmod 3$.

Evaluate f at all elements of the domain:

$$f(0) = \underline{\hspace{2cm}}$$

$$f(1) = \underline{\hspace{2cm}}$$

$$f(2) = \underline{\hspace{2cm}}$$

Problem 7.1 (11) (1 point)

Let the function $h : \mathbb{Z}_7 \rightarrow \mathbb{Z}_5$ be given by $h(x) = (4 \cdot x) \bmod 5$.

Find h evaluated at all elements of its domain.

$$h(0) = \underline{\hspace{2cm}}$$

$$h(1) = \underline{\hspace{2cm}}$$

$$h(2) = \underline{\hspace{2cm}}$$

$$h(3) = \underline{\hspace{2cm}}$$

$$h(4) = \underline{\hspace{2cm}}$$

$$h(5) = \underline{\hspace{2cm}}$$

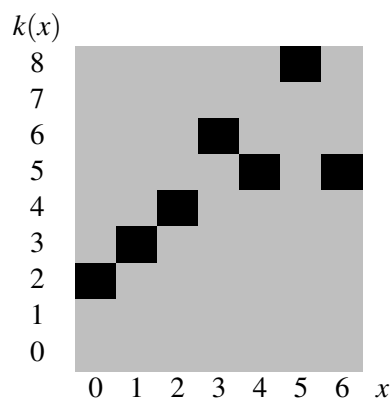
$$h(6) = \underline{\hspace{2cm}}$$

In roster form the image of A under h is $\{h(x) \mid x \in \mathbb{Z}_7\} = \{\underline{\hspace{2cm}}\}$.

In roster form the graph of h is $\{(x, h(x)) \mid x \in \mathbb{Z}_7\} = \{\underline{\hspace{2cm}}\}$.

Problem 7.1 (12) (1 point)

Suppose that the graph of the function k is given by



In roster form the graph of k is $\{(x, k(x)) \mid x \in A\} = \{\underline{\hspace{2cm}}\}$.

In roster form the domain of k is $A = \{\underline{\hspace{2cm}}\}$.

In roster form the codomain of k is $B = \{\underline{\hspace{2cm}}\}$.

In roster form the image of A under k is $\{k(x) \mid x \in A\} = \{ \rule{1.5cm}{0.4pt} \}$.

Find k evaluated at all elements of its domain.

$$k(0) = \rule{1cm}{0.4pt}$$

$$k(1) = \rule{1cm}{0.4pt}$$

$$k(2) = \rule{1cm}{0.4pt}$$

$$k(3) = \rule{1cm}{0.4pt}$$

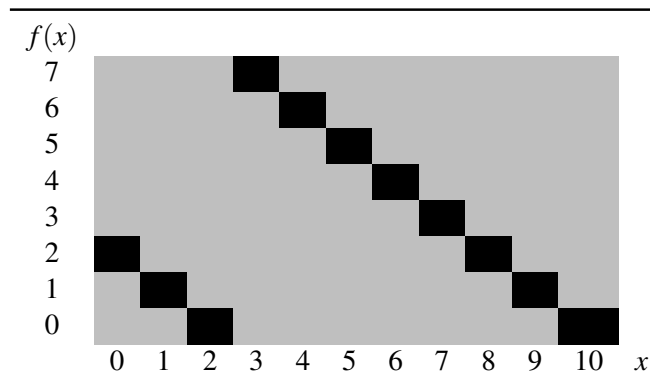
$$k(4) = \rule{1cm}{0.4pt}$$

$$k(5) = \rule{1cm}{0.4pt}$$

$$k(6) = \rule{1cm}{0.4pt}$$

Problem 7.1 (13) (1 point)

Suppose that the graph of the function f is



In roster form the domain of f is $A = \{ \rule{1.5cm}{0.4pt} \}$.

In roster form the codomain of f is $B = \{ \rule{1.5cm}{0.4pt} \}$.

In roster form the image of A under f is $\{f(x) \mid x \in A\} = \{ \rule{1.5cm}{0.4pt} \}$.

Find f evaluated at all elements of its domain.

$$f(0) = \rule{1cm}{0.4pt}$$

$$f(1) = \rule{1cm}{0.4pt}$$

$$f(2) = \underline{\hspace{1cm}}$$

$$f(3) = \underline{\hspace{1cm}}$$

$$f(4) = \underline{\hspace{1cm}}$$

$$f(5) = \underline{\hspace{1cm}}$$

$$f(6) = \underline{\hspace{1cm}}$$

$$f(7) = \underline{\hspace{1cm}}$$

$$f(8) = \underline{\hspace{1cm}}$$

$$f(9) = \underline{\hspace{1cm}}$$

$$f(10) = \underline{\hspace{1cm}}$$

Solutions

Problem 7.1 (1) *Correct Answers:*

- exactly one element
 - each element
 - domain
 - codomain
-

Problem 7.1 (2) *Correct Answers:*

- N
 - D
 - I
 - C
-

Problem 7.1 (4)

Hint: The image of A under k is:

$$\{k(x) \mid x \in \mathbb{Z}_9\} = \{k(x) \mid x \in \{0, 1, \dots, 9\}\} = \{k(0), k(1), \dots, k(8)\} = \{1, 2, \dots, 2\}$$

The graph of k is:

$$\{(x, k(x)) \mid x \in \mathbb{Z}_9\} = \{(x, k(x)) \mid x \in \{0, 1, 2, \dots, 8\}\} = \{(0, k(0)), (1, k(1)), \dots, (8, k(8))\} = \{(0, 1), (1, 2), \dots, (8, 2)\}$$

Correct Answers:

- $k(0) = 1, k(1) = 2, k(2) = 2, k(3) = 0, k(4) = 2, k(5) = 0, k(6) = 0, k(7) = 1, k(8) = 2$
 - The image of k is $\{1, 2, 0\}$
 - The graph of k is $\{(1, 2), (2, 2), (4, 2), (8, 2), (0, 1), (7, 1), (3, 0), (5, 0), (6, 0)\}$
-

Problem 7.1 (5)

Hint: The graph of the function k is the subset of the Cartesian product $\{0, 1, \dots, 4\} \times \{0, 1, \dots, 10\}$ that is represented by black pixels. Thus the graph of k is

$$\{(0, 2), (1, 6), \dots, (4, 1)\}$$

The domain of k is the set that contains all possible values for x . They are the values on the horizontal axis of the plot.

The codomain of k is the set that contains all possible values for $f(x)$. They are the values on the vertical axis of the plot.

Because the graph of k is $\{(x, k(x)) \mid x \in A\}$ we can read off the values of k evaluated at the elements of the domain from the graph and get:

$$k(0) = 6, k(1) = 6, \text{ and } k(4) = 1$$

We can also directly read these values off the plot by finding the vertical coordinate $k(x)$ of the black pixel with horizontal coordinate x .

The image of A under k is:

$$\{k(x) \mid x \in \{0, 1, \dots, 4\}\} = \{k(0), k(1), \dots, k(4)\} = \{2, 6, \dots, 1\}$$

Correct Answers:

- The graph is $\{(2, 9), (3, 9), (1, 6), (0, 2), (4, 1)\}$
- The domain is $\{0, 1, 2, 3, 4\}$
- The codomain is $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
- $k(0) = 2, k(1) = 6, k(2) = 9, k(3) = 9, (k(4) = 1$
- The image is $\{2, 6, 9, 1\}$

Problem 7.1 (6) *Correct Answers:*

- 7
- 7

Problem 7.1 (7) *Correct Answers:*

Solution:

To evaluate a function at a particular value, substitute that value for x in the function's formula and simplify.

a. $G(0) = -2(0)^2 - 3(0) + 3$
 $= -2(0) + 0 + 3$
 $= 0 + 0 + 3$
 $= 3$

b. $G(-2) = -2(-2)^2 - 3(-2) + 3$
 $= -2(4) + 6 + 3$
 $= -8 + 6 + 3$
 $= 1$

Correct Answers:

- 3
- 1

Problem 7.1 (8) *Correct Answers:*

- 5
- -5
- -5
- 0

Problem 7.1 (9) *Correct Answers:*

- 6

Problem 7.1 (10) *Correct Answers:*

- 0
- 0
- 0

Problem 7.1 (11) *Correct Answers:*

- 0
- 4
- 3
- 2
- 1
- 0
- 4
- 0, 4, 3, 2, 1
- $(1, 4), (6, 4), (2, 3), (3, 2), (4, 1), (0, 0), (5, 0)$

Problem 7.1 (12)

Hint: The graph of the function $k : A \rightarrow B$ is

$$\{(x, k(x)) \mid x \in A\} \subseteq A \times B.$$

In the plot the elements of the graph are represented by black pixels. Thus in our case:

$$\{(x, k(x)) \mid x \in A\} = \{(0, 2), (1, 3), (2, 4), \dots\}$$

Correct Answers:

- The graph is $\{(0, 2), (1, 3), (2, 4), (3, 6), (4, 5), (5, 8), (6, 5)\}$
- $A = \{0, 1, 2, 3, 4, 5, 6\}$
- $B = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$
- The image is $\{2, 3, 4, 6, 5, 8\}$
- 2
- 3
- 4
- 6
- 5
- 8
- 5

Problem 7.1 (13)

Hint: The graph of the function $f : A \rightarrow B$ is

$$\{(x, f(x)) \mid x \in A\} \subseteq A \times B.$$

In the plot the elements of the graph are represented by black pixels.

Correct Answers:

- 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10
- 0, 1, 2, 3, 4, 5, 6, 7
- 2, 1, 0, 7, 6, 5, 4, 3

- 2
- 1
- 0
- 7
- 6
- 5
- 4
- 3
- 2
- 1
- 0

Problem 7.1 (3) *Correct Answers:*

- 3
- 3
- 0

7.2 Equality of Functions

Problem 7.2 (1) (1 point)

Complete the definitions:

Let A and B be sets and $f : A \rightarrow B$ and $g : A \rightarrow B$ be functions.

We say that f and g ^(A) and write $f = g$ if ^(B) for all $a \in A$.

(A): [select: | **are equal** | **are not equal** | **are subsets** | **are not subsets** | **are composites** | **are inverses**]

(B): [select: | **f(a) is not g(a)** | $f(a) < g(a)$ | $f(a) > g(a)$ | **f(a) = g(a)**]

If f and g ^(C) , we write $f \neq g$.

(C): [select: | **are equal** | **are not equal** | **are subsets** | **are not subsets** | **are composites** | **are inverses**]

Problem 7.2 (2) (1 point)

To determine whether the functions

$f : \mathbb{Z}_8 \rightarrow \mathbb{Z}_8$, $f(x) = (x + 2) \bmod 8$ and

$g : \mathbb{Z}_8 \rightarrow \mathbb{Z}_8$, $g(x) = (x - 6) \bmod 8$

are equal, evaluate them at all points of their domain:

$f(0) = \underline{\hspace{1cm}}$ $g(0) = \underline{\hspace{1cm}}$

$f(1) = \underline{\hspace{1cm}}$ $g(1) = \underline{\hspace{1cm}}$

$f(2) = \underline{\hspace{1cm}}$ $g(2) = \underline{\hspace{1cm}}$

$f(3) = \underline{\hspace{1cm}}$ $g(3) = \underline{\hspace{1cm}}$

$f(4) = \underline{\hspace{1cm}}$ $g(4) = \underline{\hspace{1cm}}$

$f(5) = \underline{\hspace{1cm}}$ $g(5) = \underline{\hspace{1cm}}$

$$f(6) = \text{---} \quad g(6) = \text{---}$$

$$f(7) = \text{---} \quad g(7) = \text{---}$$

Now conclude whether they are equal.

The function f _____ the function g .

[select: | **is equal to** | **is not equal to**]

Problem 7.2 (3) (1 point)

To determine whether the functions

$$f : \mathbb{Z}_5 \rightarrow \mathbb{Z}_5, f(x) = (1 \cdot x) \bmod 5 \text{ and}$$

$$g : \mathbb{Z}_5 \rightarrow \mathbb{Z}_5, g(x) = (2 \cdot x) \bmod 5$$

are equal, evaluate them at all points of their domain:

$$f(0) = \text{---} \quad g(0) = \text{---}$$

$$f(1) = \text{---} \quad g(1) = \text{---}$$

$$f(2) = \text{---} \quad g(2) = \text{---}$$

$$f(3) = \text{---} \quad g(3) = \text{---}$$

$$f(4) = \text{---} \quad g(4) = \text{---}$$

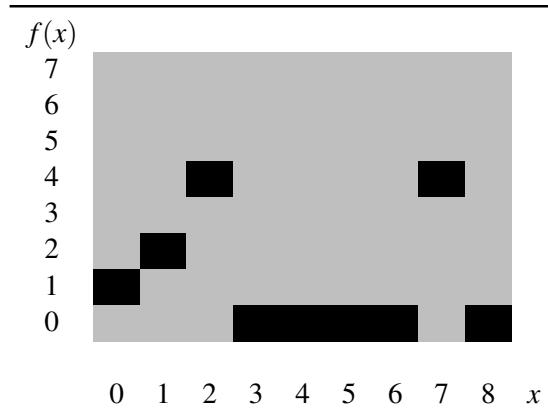
Now conclude whether they are equal.

The function f _____ the function g .

[select: | **is equal to** | **is not equal to**]

Problem 7.2 (4) (1 point)

Let $f : \mathbb{Z}_9 \rightarrow \mathbb{Z}_8$, be given by



Let $g : \mathbb{Z}_9 \rightarrow \mathbb{Z}_8$, $g(x) = 2^x \bmod 8$.

To determine whether the functions f and g are equal find:

$$f(0) = \text{---} \quad g(0) = \text{---}$$

$$f(1) = \text{---} \quad g(1) = \text{---}$$

$$f(2) = \text{---} \quad g(2) = \text{---}$$

$$f(3) = \text{---} \quad g(3) = \text{---}$$

$$f(4) = \text{---} \quad g(4) = \text{---}$$

$$f(5) = \text{---} \quad g(5) = \text{---}$$

$$f(6) = \text{---} \quad g(6) = \text{---}$$

$$f(7) = \text{---} \quad g(7) = \text{---}$$

$$f(8) = \text{---} \quad g(8) = \text{---}$$

Now conclude whether f and g are equal.

The function f ^(A) the function g , because $f(x)$ ^(B) $g(x)$ for ^(C).

(A): [select: | **is equal to** | **is not equal to**]

(B): [select: | **is equal to** | **is not equal to**]

(C): [select: | **for x=0** | **for x=1** | **for x=2** | **for x=3** | **for x=4** | **for x=5** | **for x=6** | **for x=7** | **for x=8** | **for all x in { 0, 1, 2, 3, 4, 5, 6, 7, 8 }**]

Problem 7.2 (5) (1 point)

To determine whether the functions

$$f : \mathbb{Z}_4 \rightarrow \mathbb{Z}_4, f(x) = (x + 1) \bmod 4 \text{ and}$$

$$g : \mathbb{Z}_4 \rightarrow \mathbb{Z}_4, g(x) = (x - 1) \bmod 4$$

are equal, evaluate them at all points of their domain:

$$f(0) = \text{---} \quad g(0) = \text{---}$$

$$f(1) = \text{---} \quad g(1) = \text{---}$$

$$f(2) = \text{---} \quad g(2) = \text{---}$$

$$f(3) = \text{---} \quad g(3) = \text{---}$$

Now conclude whether they are equal.

The function f _____ the function g .

[select: | **is equal to** | **is not equal to**]

Problem 7.2 (6) (1 point)

To determine whether the functions

$$f : \mathbb{Z}_7 \rightarrow \mathbb{Z}_7, f(x) = (1 \cdot x) \bmod 7 \text{ and}$$

$$g : \mathbb{Z}_7 \rightarrow \mathbb{Z}_7, g(x) = (2 \cdot x) \bmod 7$$

are equal, evaluate them at all points of their domain:

$$f(0) = \text{---} \quad g(0) = \text{---}$$

$$f(1) = \text{---} \quad g(1) = \text{---}$$

$$f(2) = \text{---} \quad g(2) = \text{---}$$

$$f(3) = \text{---} \quad g(3) = \text{---}$$

$$f(4) = \text{---} \quad g(4) = \text{---}$$

$$f(5) = \text{---} \quad g(5) = \text{---}$$

$$f(6) = \text{---} \quad g(6) = \text{---}$$

Now conclude whether they are equal.

The function f _____ the function g .

[select: | **is equal to** | **is not equal to**]

Problem 7.2 (7) (1 point)

To determine whether the functions

$$f : \mathbb{Z}_3^\otimes \rightarrow \mathbb{Z}_3^\otimes, f(x) = x^2 \bmod 3 \text{ and}$$

$$g : \mathbb{Z}_3^\otimes \rightarrow \mathbb{Z}_3^\otimes, g(x) = 1$$

are equal, evaluate them at all points of their domain:

$$f(1) = \text{---} \quad g(1) = \text{---}$$

$$f(2) = \text{---} \quad g(2) = \text{---}$$

Now conclude whether they are equal.

The function f _____ the function g .

[select: | **is equal to** | **is not equal to**]

Problem 7.2 (8) (1 point)

For each of these pairs of functions f and g decide whether f and g are equal.

When in doubt, make a table of the values of both functions under consideration for all elements in their domain.

E = Equal and N = Not equal

1. ___ $f : \mathbb{Z}_5 \rightarrow \mathbb{Z}_5, f(x) = (x+1) \bmod 5$ and $g : \mathbb{Z}_5 \rightarrow \mathbb{Z}_5, g(x) = (x-4) \bmod 5$

2. ___ $f : \mathbb{Z} \rightarrow \mathbb{Z}, f(x) = x+1$ and $g : \mathbb{Z} \rightarrow \mathbb{Z}, g(x) = x-4$

3. ___ $f : \mathbb{Z}_{10} \rightarrow \mathbb{Z}_{10}, f(x) = (x+3) \bmod 10$ and $g : \mathbb{Z}_{10} \rightarrow \mathbb{Z}_{10}, g(x) = (x-3) \bmod 10$

4. ___ $f : \mathbb{Z}_3 \rightarrow \mathbb{Z}_3, f(x) = x^2 \bmod 3$ and $g : \mathbb{Z}_3 \rightarrow \mathbb{Z}_3, g(x) = x$

Solutions

Problem 7.2 (1) *Correct Answers:*

- are equal
 - $f(a) = g(a)$
 - are not equal
-

Problem 7.2 (2) *Correct Answers:*

- 2
 - 2
 - 3
 - 3
 - 4
 - 4
 - 5
 - 5
 - 6
 - 6
 - 7
 - 7
 - 0
 - 0
 - 1
 - 1
 - is equal to
-

Problem 7.2 (3) *Correct Answers:*

- 0
 - 0
 - 1
 - 2
 - 2
 - 4
 - 3
 - 1
 - 4
 - 3
 - is not equal to
-

Problem 7.2 (4) *Correct Answers:*

Hint: The graph of the function $f : A \rightarrow B$ is

$$\{(x, f(x)) \mid x \in A\} \subseteq A \times B.$$

In the plot the elements of the graph are represented by black pixels.

Two functions $f : A \rightarrow B$ and $g : A \rightarrow B$ are equal when $f(x) = g(x)$ for all $x \in A$.

Correct Answers:

- 1
- 1
- 2
- 2
- 4
- 4
- 0
- 0
- 0
- 0
- 0
- 0
- 0
- 4
- 0
- 0
- 0
- is not equal to
- is not equal to
- for $x=7$

Problem 7.2 (5) *Correct Answers:*

- 1
- 3
- 2
- 0
- 3
- 1
- 0
- 2
- is not equal to

Problem 7.2 (6) *Correct Answers:*

- 0
- 0
- 1
- 2
- 2
- 4
- 3
- 6
- 4
- 1
- 5
- 3
- 6

- 5
- is not equal to

Problem 7.2 (7) *Correct Answers:*

- 1
- 1
- 1
- 1
- is equal to

Problem 7.2 (8) *Correct Answers:*

- E
- N
- N
- N

7.3 Composite Functions

Problem 7.3 (1) (1 point)

Complete the definitions:

Let $f : B \rightarrow C$ and $g : A \rightarrow B$ be functions.

The (A) of f and g , written $f \circ g$, is the function $f \circ g : \underline{(B)} \rightarrow \underline{(C)}$ defined by $f \circ g(x) = f(g(x))$.

(A): [select: | **subset** | **identity** | **inverse** | **composite**]

(B): [select: | **A** | **B** | **C**]

(C): [select: | **A** | **B** | **C**]

Problem 7.3 (2) (1 point)

Consider the two functions

$$f : \mathbb{Z}_3 \rightarrow \mathbb{Z}_3, f(x) = (x + 1) \bmod 3$$

and

$$g : \mathbb{Z} \rightarrow \mathbb{Z}_3, g(x) = (0) \bmod 3.$$

Evaluate:

$$g(0) = \underline{\hspace{1cm}} \quad f(g(0)) = \underline{\hspace{1cm}}$$

$$g(1) = \underline{\hspace{1cm}} \quad f(g(1)) = \underline{\hspace{1cm}}$$

$$g(2) = \underline{\hspace{1cm}} \quad f(g(2)) = \underline{\hspace{1cm}}$$

Problem 7.3 (3) (1 point)

Consider the two functions

$$f : \mathbb{Z}_5 \rightarrow \mathbb{Z}_5, f(x) = (x^5 + 4) \bmod 5$$

and

$$g : \mathbb{Z} \rightarrow \mathbb{Z}_5, g(x) = (4x^2 + 3x) \bmod 5.$$

Evaluate:

$$g(0) = \text{---} \quad f(g(0)) = \text{---}$$

$$g(1) = \text{---} \quad f(g(1)) = \text{---}$$

$$g(2) = \text{---} \quad f(g(2)) = \text{---}$$

$$g(3) = \text{---} \quad f(g(3)) = \text{---}$$

$$g(4) = \text{---} \quad f(g(4)) = \text{---}$$

Problem 7.3 (4) (1 point)

Consider the two functions

$$h : \mathbb{Z}_6 \rightarrow \mathbb{Z}_2 \text{ given by } h(x) = ((1 \cdot x^2) + 0) \bmod 2$$

and

$$m : \mathbb{Z}_6 \rightarrow \mathbb{Z}_6 \text{ given by } m(x) = ((1 \cdot x^2) + 5) \bmod 6.$$

Evaluate:

$$m(0) = \text{---} \quad (h \circ m)(0) = \text{---}$$

$$m(1) = \text{---} \quad (h \circ m)(1) = \text{---}$$

$$m(2) = \text{---} \quad (h \circ m)(2) = \text{---}$$

$$m(3) = \text{---} \quad (h \circ m)(3) = \text{---}$$

$$m(4) = \text{---} \quad (h \circ m)(4) = \text{---}$$

$$m(5) = \text{---} \quad (h \circ m)(5) = \text{---}$$

Problem 7.3 (5) (1 point)

Consider the two functions

$$g : \mathbb{Z}_4 \rightarrow \mathbb{Z}_4 \text{ given by } g(x) = (3x + 2) \bmod 4$$

and

$$h : \mathbb{Z}_4 \rightarrow \mathbb{Z}_4 \text{ given by } h(x) = (3) \bmod 4.$$

Let $f := g \circ h$.

Evaluate:

$$f(0) = \underline{\hspace{1cm}}$$

$$f(1) = \underline{\hspace{1cm}}$$

$$f(2) = \underline{\hspace{1cm}}$$

$$f(3) = \underline{\hspace{1cm}}$$

Problem 7.3 (6) (1 point)

Let $f(x) = 2x^2$, $g(x) = 6x + 2$, and $h(x) = x^2 + 4x + 2$. Find the following:

$$(f \circ g)(3) = \underline{\hspace{1cm}} \quad f(g(3)) = \underline{\hspace{1cm}}$$

$$(g \circ f)(0) = \underline{\hspace{1cm}} \quad g(f(0)) = \underline{\hspace{1cm}}$$

$$(h \circ h)(2) = \underline{\hspace{1cm}} \quad h(h(2)) = \underline{\hspace{1cm}}$$

Solutions

Problem 7.3 (1) *Correct Answers:*

- composite
 - A
 - C
-

Problem 7.3 (2) *Correct Answers:*

- 0
 - 1
 - 0
 - 1
 - 0
 - 1
-

Problem 7.3 (3) *Correct Answers:*

- 0
 - 4
 - 2
 - 1
 - 2
 - 1
 - 0
 - 4
 - 1
 - 0
-

Problem 7.3 (4) *Correct Answers:*

- 5
 - 1
 - 0
 - 0
 - 3
 - 1
 - 2
 - 0
 - 3
 - 1
 - 0
 - 0
-

Problem 7.3 (5) *Correct Answers:*

- 3
- 3
- 3
- 3

Problem 7.3 (6) *Correct Answers:*

- 800
- 800
- 2
- 2
- 254
- 254

7.4 Identity Functions

Problem 7.4 (1) (1 point)

Complete the following.

Let A be a nonempty set. The identity function on A is the function $id_A : A \rightarrow A$ given by $id_A(x) = \underline{\hspace{1cm}}$.

[select: | ? | 0 | 1 | -1 | x | -x | $\frac{1}{x}$ | $-\frac{1}{x}$]

Let B be a set and $f : A \rightarrow B$ and $g : B \rightarrow A$ be functions.

Then $(f \circ id_A)(x) = \underline{\hspace{1cm}}$.

[select: | ? | 0 | 1 | -1 | x | -x | f(x) | -f(x) | g(x) | $\frac{1}{g(x)}$ | $\frac{1}{x}$ | $-\frac{1}{x}$]

and $(id_A \circ g)(x) = \underline{\hspace{1cm}}$.

[select: | ? | 0 | 1 | -1 | x | -x | f(x) | -f(x) | g(x) | $\frac{1}{g(x)}$ | $\frac{1}{x}$ | $-\frac{1}{x}$]

Problem 7.4 (2) (1 point)

Compute:

$$0 \bmod 4 = \underline{\hspace{1cm}}$$

$$1 \bmod 4 = \underline{\hspace{1cm}}$$

$$2 \bmod 4 = \underline{\hspace{1cm}}$$

$$3 \bmod 4 = \underline{\hspace{1cm}}$$

$$4 \bmod 4 = \underline{\hspace{1cm}}$$

$$5 \bmod 4 = \underline{\hspace{1cm}}$$

$$6 \bmod 4 = \underline{\hspace{1cm}}$$

$$7 \bmod 4 = \underline{\hspace{1cm}}$$

$$8 \bmod 4 = \underline{\hspace{1cm}}$$

$$9 \bmod 4 = \underline{\hspace{1cm}}$$

Problem 7.4 (3) (1 point)

Let $f : \mathbb{Z}_7 \rightarrow \mathbb{Z}_7$ be given by $f(x) = (3x^6 + 6x^4) \bmod 7$.

Let $\text{id}_{\mathbb{Z}_7} : \mathbb{Z}_7 \rightarrow \mathbb{Z}_7$ given by $\text{id}_{\mathbb{Z}_7}(x) = x$ be the identity function on $\mathbb{Z}_7$.

Evaluate f and $\text{id}_{\mathbb{Z}_7}$ at all elements of the domain:

$$f(0) = \text{---} \quad \text{id}_{\mathbb{Z}_7}(0) = \text{---}$$

$$f(1) = \text{---} \quad \text{id}_{\mathbb{Z}_7}(1) = \text{---}$$

$$f(2) = \text{---} \quad \text{id}_{\mathbb{Z}_7}(2) = \text{---}$$

$$f(3) = \text{---} \quad \text{id}_{\mathbb{Z}_7}(3) = \text{---}$$

$$f(4) = \text{---} \quad \text{id}_{\mathbb{Z}_7}(4) = \text{---}$$

$$f(5) = \text{---} \quad \text{id}_{\mathbb{Z}_7}(5) = \text{---}$$

$$f(6) = \text{---} \quad \text{id}_{\mathbb{Z}_7}(6) = \text{---}$$

Now determine whether f is equal to $\text{id}_{\mathbb{Z}_7}$.

The function f _____ to $\text{id}_{\mathbb{Z}_7}$.

[select: | **is equal** | **is NOT equal**]

Problem 7.4 (4) (1 point)

Let $f : \mathbb{Z}_5 \rightarrow \mathbb{Z}_5$, $f(x) = (4x^3 + 2x) \bmod 5$.

Evaluate f at all elements of the domain:

$$f(0) = \text{---} \quad \text{id}_{\mathbb{Z}_5}(0) = 0$$

$$f(1) = \text{---} \quad \text{id}_{\mathbb{Z}_5}(1) = 1$$

$$f(2) = \text{---} \quad \text{id}_{\mathbb{Z}_5}(2) = 2$$

$$f(3) = \text{---} \quad \text{id}_{\mathbb{Z}_5}(3) = 3$$

$$f(4) = \text{---} \quad \text{id}_{\mathbb{Z}_5}(4) = 4$$

Now determine whether f is equal to the identity function $id_{\mathbb{Z}_5}$. For your convenience the values of $id_{\mathbb{Z}_5}$ at all elements of its domain are also given above.

The function f _____ on $\mathbb{Z}_5$.

[select: | **is the identity function** | **is NOT the identity function**]

Problem 7.4 (5) (1 point)

Let $f : \mathbb{Z}_3 \rightarrow \mathbb{Z}_3$, $f(x) = (x^2) \bmod 3$.

Evaluate f at all elements of the domain:

$f(0) = \underline{\hspace{1cm}}$

$f(1) = \underline{\hspace{1cm}}$

$f(2) = \underline{\hspace{1cm}}$

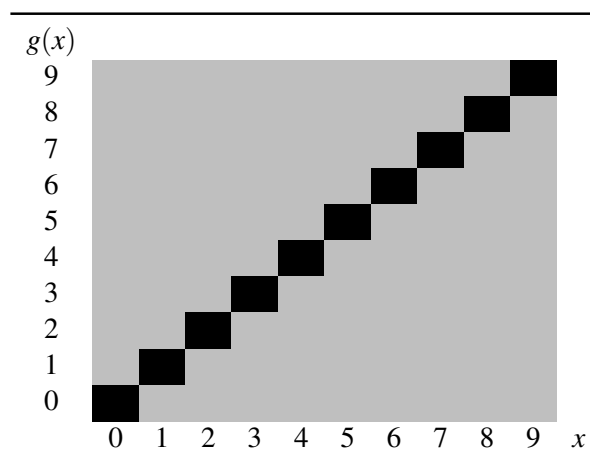
Now conclude whether f is equal to the identity function on $\mathbb{Z}_3$.

The function f _____ on $\mathbb{Z}_3$.

[select: | **is the identity function** | **is NOT the identity function**]

Problem 7.4 (6) (1 point)

Suppose that the graph of the function g is



In roster form the domain of g is $A = \{ \underline{\hspace{2cm}} \}$.

In roster form the codomain of g is $B = \{ \text{_____} \}$.

In roster form the image of A under g is $\{g(x) \mid x \in A\} = \{ \text{_____} \}$.

Find g evaluated at all elements of its domain.

$$g(0) = \text{_____}$$

$$g(1) = \text{_____}$$

$$g(2) = \text{_____}$$

$$g(3) = \text{_____}$$

$$g(4) = \text{_____}$$

$$g(5) = \text{_____}$$

$$g(6) = \text{_____}$$

$$g(7) = \text{_____}$$

$$g(8) = \text{_____}$$

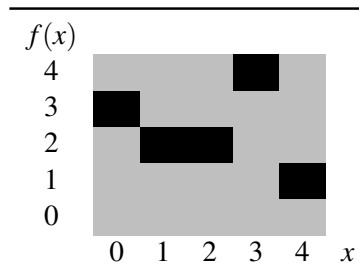
$$g(9) = \text{_____}$$

The function g is _____.

[select: | **the identity function** | **not the identity function**]

Problem 7.4 (7) (1 point)

Suppose that the graph of the function f is



In roster form the domain of f is $A = \{ \text{_____} \}$.

In roster form the codomain of f is $B = \{ \text{_____} \}$.

In roster form the image of A under f is $\{f(x) \mid x \in A\} = \{ \text{_____} \}$.

Find f evaluated at all elements of its domain.

$$f(0) = \text{_____}$$

$$f(1) = \text{_____}$$

$$f(2) = \text{_____}$$

$$f(3) = \text{_____}$$

$$f(4) = \underline{\hspace{1cm}}$$

The function f is _____.

[select: | **the identity function** | **not the identity function**]

Solutions

Problem 7.4 (1) *Correct Answers:*

- x
 - $f(x)$
 - $g(x)$
-

Problem 7.4 (2) *Correct Answers:*

- 0
 - 1
 - 2
 - 3
 - 0
 - 1
 - 2
 - 3
 - 0
 - 1
-

Problem 7.4 (3) *Correct Answers:*

- 0
- 0
- 2
- 1
- 1
- 2
- 6
- 3
- 6
- 4
- 1
- 5
- 2
- 6
- is NOT equal

Problem 7.4 (4) Correct Answers:

- 0
- 1
- 1
- 4
- 4
- is NOT the identity function

Problem 7.4 (5) Correct Answers:

- 0
- 1
- 1
- is NOT the identity function

Problem 7.4 (6) Correct Answers:

Hint: The graph of the function $g : A \rightarrow B$ is

$$\{(x, g(x)) \mid x \in A\} \subseteq A \times B.$$

In the plot the elements of the graph are represented by black pixels.

The function g is the identity function on A when $B = A$ and $g(x) = x$ for all $x \in A$.

Correct Answers:

- 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
- 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
- 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
- 0
- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- the identity function

Problem 7.4 (7) Correct Answers:

Hint: The graph of the function $f : A \rightarrow B$ is

$$\{(x, f(x)) \mid x \in A\} \subseteq A \times B.$$

In the plot the elements of the graph are represented by black pixels.

The function f is the identity function on A when $B = A$ and $f(x) = x$ for all $x \in A$.

Correct Answers:

- 0, 1, 2, 3, 4
- 0, 1, 2, 3, 4
- 3, 2, 4, 1
- 3
- 2
- 2
- 4
- 1
- not the identity function

7.5 Inverse Functions

Problem 7.5 (1) (1 point)

Complete the following:

Definition. Let $f : A \rightarrow B$ be a function.

We say f is invertible if (A) element (B), (C) element (D) such that (E).

(A): [select: | **for every** | **there is exactly one** | **for one**]

(B): [select: | **a in A** | **b in B**]

(C): [select: | **for every** | **there is exactly one** | **for one**]

(D): [select: | **a in A** | **b in B**]

(E): [select: | **f(a) = b** | **f(b) = a** | **f(a) = 1**]

Definition. The inverse function $f^{-1} : \underline{(A)}$ of an invertible function $f : A \rightarrow B$ is the function that assigns to each element (B) the unique element (C) such that (D).

(A): [select: | $A \rightarrow B$ | $B \rightarrow A$]

(B): [select: | **a in A** | **b in B**]

(C): [select: | **a in A** | **b in B**]

(D): [select: | **f(a) = b** | **f(b) = a** | **f(a) = 1**]

Theorem. If a function $f : \underline{\hspace{1cm}}$ is invertible and $f^{-1} : B \rightarrow A$ is its inverse, then f is the inverse of f^{-1} .

[select: | $A \rightarrow B$ | $B \rightarrow A$]

Theorem. Let $f : A \rightarrow B$ be a function and let $f^{-1} : \underline{(A)}$ be its inverse, The function $f \circ f^{-1}$ is the $\underline{(B)}$.
The function $f^{-1} \circ f$ is the $\underline{(C)}$.

(A): [select: | $A \rightarrow B$ | $B \rightarrow A$]

(B): [select: | **identity function on A** | **identity function on B**]

(C): [select: | **identity function on A** | **identity function on B**]

Problem 7.5 (2) (1 point)

Consider the function $g : \{8, 9, \dots, 16, 17\} \rightarrow \{8, 9, \dots, 16, 17\}$ given by

x	8	9	10	11	12	13	14	15	16	17
$g(x)$	9	11	12	17	8	16	14	13	15	17

Is the function g invertible ?
___ (Y or N)

If g is invertible find $g^{-1}(17)$. If g is not invertible leave the field empty.
 $g^{-1}(17) = \underline{\hspace{2cm}}$

Problem 7.5 (3) (1 point)

Consider the function

$\varphi : \{-8, -7, \dots, 0, 1\} \rightarrow \{-8, -7, \dots, 0, 1\}$

x	-8	-7	-6	-5	-4	-3	-2	-1	0	1
$\varphi(x)$	1	-6	0	-4	-3	-8	-2	-7	-5	-1

Is the function $\varphi(x)$ invertible? ___ (Y or N)

Problem 7.5 (4) (1 point)

Assume that the function f is invertible. Denote the inverse of f by f^{-1} .

If $f(8) = 5$ then $f^{-1}(5) = \underline{\hspace{1cm}}$.

If $f^{-1}(-5) = -9$ then $f(-9) = \underline{\hspace{1cm}}$.

Problem 7.5 (5) (1 point)

Let $f : \mathbb{Z}_2 \rightarrow \mathbb{Z}_2$, $f(x) = (x) \bmod 2$.

Evaluate f at all elements of its domain.

$f(0) = \underline{\hspace{1cm}}$

$f(1) = \underline{\hspace{1cm}}$

Thus the function f _____.

[select: | **is invertible** | **is not invertible**]

Problem 7.5 (6) (1 point)

Consider the function $g : \{-3, -2, \dots, 5, 6\} \rightarrow \{-3, -2, \dots, 5, 6\}$ given by

x	-3	-2	-1	0	1	2	3	4	5	6
$g(x)$	0	-3	2	3	1	-1	-2	6	5	0

Is the function g invertible ? $\underline{\hspace{1cm}}$ (Y or N)

Problem 7.5 (7) (1 point)

Let $f : \mathbb{Z}_{11} \rightarrow \mathbb{Z}_{11}$, $f(x) = (6x) \bmod 11$. Evaluate f at all elements of the domain:

$f(0) = \underline{\hspace{1cm}}$

$f(1) = \underline{\hspace{1cm}}$

$f(2) = \underline{\hspace{1cm}}$

$f(3) = \underline{\hspace{1cm}}$

$f(4) = \underline{\hspace{1cm}}$

$f(5) = \underline{\hspace{1cm}}$

$f(6) = \underline{\hspace{1cm}}$

$$f(7) = \underline{\hspace{1cm}}$$

$$f(8) = \underline{\hspace{1cm}}$$

$$f(9) = \underline{\hspace{1cm}}$$

$$f(10) = \underline{\hspace{1cm}}$$

The function f is invertible. Find the image of the inverse f^{-1} of f at all elements of its domain.

$$f^{-1}(0) = \underline{\hspace{1cm}}$$

$$f^{-1}(1) = \underline{\hspace{1cm}}$$

$$f^{-1}(2) = \underline{\hspace{1cm}}$$

$$f^{-1}(3) = \underline{\hspace{1cm}}$$

$$f^{-1}(4) = \underline{\hspace{1cm}}$$

$$f^{-1}(5) = \underline{\hspace{1cm}}$$

$$f^{-1}(6) = \underline{\hspace{1cm}}$$

$$f^{-1}(7) = \underline{\hspace{1cm}}$$

$$f^{-1}(8) = \underline{\hspace{1cm}}$$

$$f^{-1}(9) = \underline{\hspace{1cm}}$$

$$f^{-1}(10) = \underline{\hspace{1cm}}$$

Problem 7.5 (8) (1 point)

Let $f : \mathbb{Z}_6 \rightarrow \mathbb{Z}_6$, $f(x) = (1 + x) \bmod 6$.

Evaluate f at all elements of the domain:

$$f(0) = \underline{\hspace{1cm}}$$

$$f(1) = \underline{\hspace{1cm}}$$

$$f(2) = \underline{\hspace{1cm}}$$

$$f(3) = \underline{\hspace{1cm}}$$

$$f(4) = \underline{\hspace{2cm}}$$

$$f(5) = \underline{\hspace{2cm}}$$

The function f is invertible. Find the image of the inverse f^{-1} of f at all elements of its domain.

$$f^{-1}(0) = \underline{\hspace{2cm}}$$

$$f^{-1}(1) = \underline{\hspace{2cm}}$$

$$f^{-1}(2) = \underline{\hspace{2cm}}$$

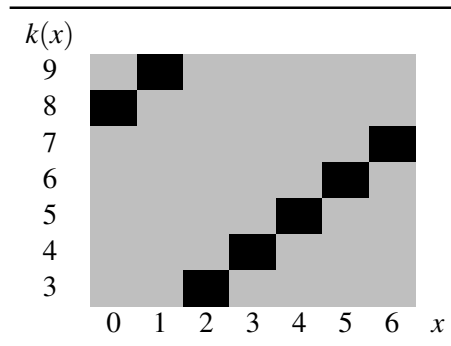
$$f^{-1}(3) = \underline{\hspace{2cm}}$$

$$f^{-1}(4) = \underline{\hspace{2cm}}$$

$$f^{-1}(5) = \underline{\hspace{2cm}}$$

Problem 7.5 (9) (1 point)

Suppose that the graph of the function k is



In roster form the domain of k is $A = \{ \underline{\hspace{2cm}} \}$.

In roster form the codomain of k is $B = \{ \underline{\hspace{2cm}} \}$.

Find k evaluated at all elements of its domain.

$$k(0) = \underline{\hspace{2cm}}$$

$$k(1) = \underline{\hspace{2cm}}$$

$$k(2) = \underline{\hspace{2cm}}$$

$$k(3) = \underline{\hspace{2cm}}$$

$$k(4) = \underline{\hspace{2cm}}$$

$$k(5) = \underline{\hspace{2cm}}$$

$$k(6) = \underline{\hspace{2cm}}$$

In roster form the image of A under k is $\{k(x) \mid x \in A\} = \{\underline{\hspace{3cm}}\}$.

The function k is .

[select: | **the identity function on A** | **not the identity function on A**]

The function k is .

[select: | **invertible** | **not invertible**]

If the function k is invertible complete the following. Otherwise leave the fields empty.

In roster form the domain of the inverse k^{-1} of k is $\{\underline{\hspace{3cm}}\}$.

In roster form the codomain of k^{-1} is $\{\underline{\hspace{3cm}}\}$.

Give the preimages of all elements of the codomain.

$$k^{-1}(3) = \underline{\hspace{2cm}}$$

$$k^{-1}(4) = \underline{\hspace{2cm}}$$

$$k^{-1}(5) = \underline{\hspace{2cm}}$$

$$k^{-1}(6) = \underline{\hspace{2cm}}$$

$$k^{-1}(7) = \underline{\hspace{2cm}}$$

$$k^{-1}(8) = \underline{\hspace{2cm}}$$

$$k^{-1}(9) = \underline{\hspace{2cm}}$$

Problem 7.5 (10) (1 point)

Determine which of these functions are invertible.

When in doubt, make a table of the values of the functions for all elements in its domain and then determine whether it is invertible.

1. $f : \mathbb{Z}_5 \rightarrow \mathbb{Z}_5, f(x) = (x+2) \bmod 5$
2. $f : \mathbb{Z}_{10} \rightarrow \mathbb{Z}_{10}, f(x) = (2 \cdot x) \bmod 10$
3. $f : \mathbb{Z}_7 \rightarrow \mathbb{Z}_7, f(x) = (x^3) \bmod 7$
4. $f : \mathbb{Z}_5 \rightarrow \mathbb{Z}_5, f(x) = (x^3) \bmod 5$

Problem 7.5 (11) (1 point)

Let $S := \{1, 2, 3, 4, 5\}$ and let $g : S \rightarrow S$ be given by the following table of values.

y	1	2	3	4	5
$g(y)$	1	3	5	4	2

Use the table to fill in the missing values. There may be more than one correct answer, in which case you should enter your answers as a comma separated list. If there are no correct answers, enter *NONE*. help (numbers)

$$g(3) = \underline{\hspace{1cm}}$$

$$g(2) = \underline{\hspace{1cm}}$$

$$g^{-1}(3) = \underline{\hspace{1cm}}$$

$$g^{-1}(2) = \underline{\hspace{1cm}}$$

Solutions

Problem 7.5 (1) *Correct Answers:*

- for every
 - $b \in B$
 - there is exactly one
 - $a \in A$
 - $f(a)=b$
 - $B \rightarrow A$
 - $b \in B$
 - $a \in A$
 - $f(a)=b$
 - $A \rightarrow B$
 - $B \rightarrow A$
 - identity function on B
 - identity function on A
-

Problem 7.5 (2) *Correct Answers:*

- N
 -
-

Problem 7.5 (3) *Correct Answers:*

- Y
-

Problem 7.5 (4) *Correct Answers:*

- 8
 - -5
-

Problem 7.5 (5) *Correct Answers:*

- 0
 - 1
 - is invertible
-

Problem 7.5 (6) *Correct Answers:*

- N
-

Problem 7.5 (7) *Correct Answers:*

- 0
- 6
- 1
- 7
- 2
- 8
- 3
- 9

- 4
- 10
- 5
- 0
- 2
- 4
- 6
- 8
- 10
- 1
- 3
- 5
- 7
- 9

Problem 7.5 (8) *Correct Answers:*

- 1
- 2
- 3
- 4
- 5
- 0
- 5
- 0
- 1
- 2
- 3
- 4

Problem 7.5 (9) *Correct Answers:*

Hint: The graph of the function $k : A \rightarrow B$ is

$$\{(x, k(x)) \mid x \in A\} \subseteq A \times B.$$

In the plot the elements of the graph are represented by black pixels.

The function k is the identity function on A when $B = A$ and $k(x) = x$ for all $x \in A$.

The function k is invertible when for each $y \in B$ there is a unique $x \in A$ such that $k(x) = y$.

Correct Answers:

- The domain of k is $A = \{0, 1, 2, 3, 4, 5, 6\}$
- The codomain of k is $B = \{3, 4, 5, 6, 7, 8, 9\}$
- $k(0) = 8$
- $k(1) = 9$
- $k(2) = 3$
- $k(3) = 4$
- $k(4) = 5$

- $k(5) = 6$
- $k(6) = 7$
- The image of A under k is $\{8, 9, 3, 4, 5, 6, 7\}$
- f is not the identity function on A .
- k is invertible.
- The domain of k^{-1} is $\{3, 4, 5, 6, 7, 8, 9\}$.
- The codomain of k^{-1} is $\{0, 1, 2, 3, 4, 5, 6\}$
- $k^{-1}(3) = 2$
- $k^{-1}(4) = 3$
- $k^{-1}(5) = 4$
- $k^{-1}(6) = 5$
- $k^{-1}(7) = 6$
- $k^{-1}(8) = 0$
- $k^{-1}(9) = 1$

Problem 7.5 (10) *Correct Answers:*

- I
- N
- N
- I

Problem 7.5 (11) *Correct Answers:*

- 5
- 3
- 2
- 5

Chapter 8

Codes

1. Character Encoding
2. Symmetric Key Cryptography
3. Caesar Ciphers
4. Other Substitution Ciphers
5. Frequency Analysis

8.1 Character Encoding

Problem 8.1 (1) (1 point)

We encode sequences of characters with the function

$$C : \{-, a, b, c, \dots, z\} \rightarrow \{0, 1, 2, 3, \dots, 26\}, C(-) = 0, C(a) = 1, \dots, C(z) = 26.$$

Decode the sequence of integers into a string using the inverse of the encoding function C :

20, 18, 1, 9, 20, 15, 18

Problem 8.1 (2) (1 point)

Let

$$C : \{-, a, b, c, \dots, z\} \rightarrow \{0, 1, 2, 3, \dots, 26\}, C(-) = 0, C(a) = 1, \dots, C(z) = 26.$$

Encode the word into a sequence of integers, separated by commas, using the function C :

traveler

Problem 8.1 (3) (1 point)

We encode sequences of characters with the function

$$C : \{-, a, b, c, \dots, z\} \rightarrow \{0, 1, 2, 3, \dots, 26\}, C(-) = 0, C(a) = 1, \dots, C(z) = 26.$$

Decode the sequence of integers into a string using the inverse of the encoding function C :

19, 16, 1, 3, 5

Problem 8.1 (4) (1 point)

Let

$$C : \{-, a, b, c, \dots, z\} \rightarrow \{0, 1, 2, 3, \dots, 26\}, C(-) = 0, C(a) = 1, \dots, C(z) = 26.$$

Encode the word into a sequence of integers, separated by commas, using the function C :

traveler

Problem 8.1 (5) (1 point)

We encode sequences of characters with the function

$$C : \{-, a, b, c, \dots, z\} \rightarrow \{0, 1, 2, 3, \dots, 26\}, C(-) = 0, C(a) = 1, \dots, C(z) = 26.$$

Decode the sequence of integers into a string using the inverse of the encoding function C :

1, 12, 5, 18, 20

Problem 8.1 (6) (1 point)

Let

$$C : \{-, a, b, c, \dots, z\} \rightarrow \{0, 1, 2, 3, \dots, 26\}, C(-) = 0, C(a) = 1, \dots, C(z) = 26.$$

Encode the word into a sequence of integers, separated by commas, using the function C :

traveler

Problem 8.1 (7) (1 point)

Find the quotient and remainder:

$$55 \text{ div } 3 = \underline{\hspace{1cm}}$$

$$55 \text{ mod } 3 = \underline{\hspace{1cm}}$$

Solutions

Problem 8.1 (1) *Correct Answers:*

Solution:

The decoded word is:

traitor

Correct Answers:

- traitor
-

Problem 8.1 (2) *Correct Answers:*

- 20, 18, 1, 22, 5, 12, 5, 18
-

Problem 8.1 (3) *Correct Answers:*

Solution:

The decoded word is:

space

Correct Answers:

- space
-

Problem 8.1 (4) *Correct Answers:*

- 20, 18, 1, 22, 5, 12, 5, 18
-

Problem 8.1 (5) *Correct Answers:*

Solution:

The decoded word is:

alert

Correct Answers:

- alert
-

Problem 8.1 (6) *Correct Answers:*

- 20, 18, 1, 22, 5, 12, 5, 18
-

Problem 8.1 (7) *Correct Answers:*

- 18
- 1

8.2 Symmetric Key Cryptography

Problem 8.2 (1) (1 point)

Complete the following.

In description of cryptographic protocols:

____^(A) sends a message to ____^(B).

(A): [select: | **Alice** | **Bob** | **Eve** | **Oscar**]

(B): [select: | **Alice** | **Bob** | **Eve** | **Oscar**]

____^(C) eavesdrops on the communication between ____^(D) and ____^(E)

(C): [select: | **Alice** | **Bob** | **Eve** | **Oscar**]

(D): [select: | **Alice** | **Bob** | **Eve** | **Oscar**]

(E): [select: | **Alice** | **Bob** | **Eve** | **Oscar**]

Problem 8.2 (2) (1 point)

Complete the following.

In a symmetric encryption protocol ____^(A) and ____^(B) agree on an encryption method, a decryption method, and a key that is used for encryption and decryption.

(A): [select: | **Alice** | **Bob** | **Eve** | **Oscar**]

(B): [select: | **Alice** | **Bob** | **Eve** | **Oscar**]

____^(C) encrypts a message using the encryption method and the key. She sends the encrypted message to ____^(D).

(C): [select: | **Alice** | **Bob** | **Eve** | **Oscar**]

(D): [select: | **Alice** | **Bob** | **Eve** | **Oscar**]

____^(E) receives the message from ____^(F) and decrypts the message using the decryption method and the key.

(E): [select: | **Alice** | **Bob** | **Eve** | **Oscar**]

(F): [select: | **Alice** | **Bob** | **Eve** | **Oscar**]

Problem 8.2 (3) (1 point)

Find the quotients and remainders:

$89470 \div 1256 = \underline{\hspace{2cm}}$ and

$89470 \bmod 1256 = \underline{\hspace{2cm}}$

$87435 \div 2349 = \underline{\hspace{2cm}}$ and

$87435 \bmod 2349 = \underline{\hspace{2cm}}$

$61352 \div 1845 = \underline{\hspace{2cm}}$ and

$61352 \bmod 1845 = \underline{\hspace{2cm}}$

$5687 \div 2960 = \underline{\hspace{2cm}}$ and

$5687 \bmod 2960 = \underline{\hspace{2cm}}$

Solutions

Problem 8.2 (1) *Correct Answers:*

- Alice
 - Bob
 - Eve
 - Alice
 - Bob
-

Problem 8.2 (2) *Correct Answers:*

- Alice
 - Bob
 - Alice
 - Bob
 - Bob
 - Alice
-

Problem 8.2 (3) *Correct Answers:*

- 71
- 294
- 37
- 522
- 33
- 467
- 1
- 2727

8.3 Caesar Ciphers

Problem 8.3 (1) (1 point)

We represent the character space by $\mathbb{A}$.

For their secure communication Alice and Bob use a Caesar Cipher shifting by 2 characters. Alice sends an encrypted message to Bob:

qspc

To decrypt the message Bob uses the **decryption** function $D : \mathbb{A} \rightarrow \mathbb{A}$ given by

$D(-) = ______$,

$D(a) = ______$,

$D(b) = ______$,

$D(c) = ______$,

$D(d) = ______$,

$D(e) = ______$,

$D(f) = ______$,

$D(g) = ______$,

$D(h) = ______$,

$D(i) = ______$,

$D(j) = ______$,

$D(k) = ______$,

$D(l) = ______$,

$D(m) = ______$,

$D(n) = ______$,

$D(o) = ______$,

$D(p) = ______$,

$D(q) = ______$,

$D(r) = ______$,

$D(s) = ______$,

$D(t) = ______$,

$D(u) = ______$,

$D(v) = ______$,

$D(w) = ______$,

$D(x) = ______$,

$D(y) = ______$,

$D(z) = ______$,

Using the function D Bob decrypts the message and obtains:

Problem 8.3 (2) (1 point)

We write $_$ for the character space. Decrypt the message that was encrypted with the Caesar cipher shifting by 2 characters.

cvcpagqc

Problem 8.3 (3) (1 point)

We represent the character space by $_$.

For their secure communication Alice and Bob use a Caesar Cipher shifting by 3 characters. Alice wants to send the following message to Bob.

dog

Alice uses the **encryption** function $E : \mathbb{A} \rightarrow \mathbb{A}$ given by:

$E(_) = _,$
 $E(a) = _,$
 $E(b) = _,$
 $E(c) = _,$
 $E(d) = _,$
 $E(e) = _,$
 $E(f) = _,$
 $E(g) = _,$
 $E(h) = _,$
 $E(i) = _,$
 $E(j) = _,$
 $E(k) = _,$
 $E(l) = _,$
 $E(m) = _,$
 $E(n) = _,$
 $E(o) = _,$
 $E(p) = _,$
 $E(q) = _,$
 $E(r) = _,$
 $E(s) = _,$
 $E(t) = _,$
 $E(u) = _,$
 $E(v) = _,$
 $E(w) = _,$
 $E(x) = _,$
 $E(y) = _,$
 $E(z) = _,$

Using the function E Alice encrypts the message and obtains:

Problem 8.3 (4) (1 point)

We write — for the character space. Encrypt the word with the Caesar cipher shifting by 4 characters.

beautiful

Problem 8.3 (5) (1 point)

We write — for the character space. Decrypt the message that was encrypted with the Caesar cipher shifting by 10 characters.

ehzxzd

Problem 8.3 (6) (1 point)

We write — for the character space. Encrypt the word with the Caesar cipher shifting by 4 characters.

binary

Problem 8.3 (7) (1 point)

Find the quotient and remainder:

$$35 \text{ div } 50 = \underline{\hspace{1cm}}$$

$$35 \text{ mod } 50 = \underline{\hspace{1cm}}$$

Solutions

Problem 8.3 (1) *Correct Answers:*

- 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
- -
- a
- sure

Problem 8.3 (2) *Correct Answers:*

- exercise

Problem 8.3 (3) *Correct Answers:*

- x
- y
- z
- -
- a
- b
- c
- d
- e
- f
- g

- h
- i
- j
- k
- l
- m
- n
- o
- p
- q
- r
- s
- t
- u
- v
- w
- ald

Problem 8.3 (4) *Correct Answers:*

- yaxqpebqh

Problem 8.3 (5) *Correct Answers:*

- origin

Problem 8.3 (6) *Correct Answers:*

- yejxnu

Problem 8.3 (7) *Correct Answers:*

- 0
- 35

8.4 Other Substitution Ciphers

Problem 8.4 (1) (1 point)

Let $f : \mathbb{Z}_4 \rightarrow \mathbb{Z}_4$, $f(x) = (2 + x) \bmod 4$.

Evaluate f at all elements of the domain:

$$f(0) = \underline{\hspace{1cm}}$$

$$f(1) = \underline{\hspace{1cm}}$$

$$f(2) = \underline{\hspace{1cm}}$$

$$f(3) = \underline{\hspace{1cm}}$$

The function f is invertible. Find the image of the inverse f^{-1} of f at all elements of its domain.

$$f^{-1}(0) = \underline{\hspace{1cm}}$$

$$f^{-1}(1) = \underline{\hspace{1cm}}$$

$$f^{-1}(2) = \underline{\hspace{1cm}}$$

$$f^{-1}(3) = \underline{\hspace{1cm}}$$

Problem 8.4 (2) (1 point)

Bob receives an encrypted message from Alice:

htklslxfkx

First he applies the encoding function

$$C : \{-, a, b, c, \dots, z\} \rightarrow \{0, 1, 2, 3, \dots, 26\}, C(-) = 0, C(a) = 1, \dots, C(z) = 26.$$

to each character of the encrypted message and obtains a sequence of integers:

Then Bob applies the decryption function

$$D : \{0, 1, 2, 3, \dots, 26\} \rightarrow \{-, a, b, c, \dots, z\}, D(x) = (x - 19) \bmod 27.$$

to each of those numbers. He gets the sequence of integers:

Turning the integers back into characters using the inverse of the function C he obtains the plain text (where the character space is represented by $-$):

Problem 8.4 (3) (1 point)

Alice wants to send this message to Bob:

world

First Alice applies the encoding function

$$C : \{-, a, b, c, \dots, z\} \rightarrow \{0, 1, 2, 3, \dots, 26\}, C(-) = 0, C(a) = 1, \dots, C(z) = 26.$$

She obtains a sequence of integers:

Then Alice encrypts the message using the encryption function

$$E : \{0, 1, 2, 3, \dots, 26\} \rightarrow \{0, 1, 2, 3, \dots, 26\} E(x) = (x + 14) \bmod 27.$$

She gets the sequence of integers:

For transmission she converts the integers back into characters (write $-$ for the character space) using the inverse of the function C :

Problem 8.4 (4) (1 point)

Alice and Bob meet and agree to use the code

$$C : \{-, a, b, c, \dots, z\} \rightarrow \{0, 1, 2, 3, \dots, 26\}, C(-) = 0, C(a) = 1, \dots, C(z) = 26.$$

to map characters to integers and to use the function

$$E : \{0, 1, 2, 3, \dots, 26\} \rightarrow \{0, 1, 2, 3, \dots, 26\}, E(x) = (x + 18) \bmod 27$$

for encryption. The inverse of the function E is

$$E^{-1} : \{0, 1, 2, \dots, 26\} \rightarrow \{0, 1, 2, \dots, 26\}, E^{-1}(x) = (x - 18) \bmod 27$$

They also agree to send their messages as sequences of integers.

Alice wants to send Bob the secret message:

toad

She encodes the characters with the function and obtains:

$$C(t) = _, C(o) = _, C(a) = _, C(d) = _.$$

She encrypts these with the function E and gets

$$E(C(t)) = _, E(C(o)) = _, E(C(a)) = _, E(C(d)) = _.$$

Alice sends these integers to Bob.

Bob receives the message and evaluates the function E^{-1} at the integers send by Alice:

$$E^{-1}(E(C(t))) = _, E^{-1}(E(C(o))) = _, E^{-1}(E(C(a))) = _, E^{-1}(E(C(d))) = _.$$

An application of C^{-1} yields:

$$C^{-1}(E^{-1}(E(C(t)))) = _, C^{-1}(E^{-1}(E(C(o)))) = _, C^{-1}(E^{-1}(E(C(a)))) = _, C^{-1}(E^{-1}(E(C(d)))) = _.$$

Problem 8.4 (5) (1 point)

Alice and Bob meet and agree to use the code

$$C : \{-, a, b, c, \dots, z\} \rightarrow \{0, 1, 2, 3, \dots, 26\}, C(-) = 0, C(a) = 1, \dots, C(z) = 26.$$

to map characters to integers and to use the function

$$E : \{0, 1, 2, 3, \dots, 26\} \rightarrow \{0, 1, 2, 3, \dots, 26\} E(x) = ((7 \cdot x) + 5) \bmod 27$$

for encryption. The inverse of the function E is

$$E^{-1} : \{0, 1, 2, \dots, 26\} \rightarrow \{0, 1, 2, \dots, 26\} E^{-1}(x) = ((4 \cdot x) + 7) \bmod 27.$$

They also agree to send their messages as sequences of integers.

Alice wants to send Bob the secret message:

form

She encodes the characters with the function and obtains:

$$C(f) = _, C(o) = _, C(r) = _, C(m) = _.$$

She encrypts these with the function E and gets

$$E(C(f)) = _, E(C(o)) = _, E(C(r)) = _, E(C(m)) = _.$$

Alice sends these integers to Bob.

Bob receives the message and evaluates the function E^{-1} at the integers send by Alice:

$$E^{-1}(E(C(f))) = _, E^{-1}(E(C(o))) = _, E^{-1}(E(C(r))) = _, E^{-1}(E(C(m))) = _.$$

An application of C^{-1} yields:

$$C^{-1}(E^{-1}(E(C(f)))) = _, C^{-1}(E^{-1}(E(C(o)))) = _, C^{-1}(E^{-1}(E(C(r)))) = _, C^{-1}(E^{-1}(E(C(m)))) = _$$

Bob has decrypted the secret message:

Problem 8.4 (6) (1 point)

Bob receives an encrypted message from Alice:

ogdcsjt

First he applies the encoding function

$$C : \{-, a, b, c, \dots, z\} \rightarrow \{0, 1, 2, 3, \dots, 26\}, C(-) = 0, C(a) = 1, \dots, C(z) = 26.$$

and obtains this sequence of integers:

Bob decrypts the message using the decryption function

$$D : \{0, 1, 2, 3, \dots, 26\} \rightarrow \{0, 1, 2, 3, \dots, 26\} D(x) = (14 \cdot (x - 4)) \bmod 27.$$

He gets the sequence of integers:

Applying the inverse of the encoding function C Bob obtains the plain text:

Problem 8.4 (7) (1 point)

Alice wants to send this message to Bob:

green – alert

First she applies the encoding function

$$C : \{-, a, b, c, \dots, z\} \rightarrow \{0, 1, 2, 3, \dots, 26\}, C(-) = 0, C(a) = 1, \dots, C(z) = 26.$$

and obtains this sequence of integers:

Then Alice encrypts the message using the encryption function

$$E : \{0, 1, 2, 3, \dots, 26\} \rightarrow \{0, 1, 2, 3, \dots, 26\}, E(x) = (4 \cdot x + 5) \bmod 27.$$

She gets the sequence of integers:

For transmission she converts the integers back into characters using the inverse of the function C:

Solutions

Problem 8.4 (1) *Correct Answers:*

- 2
 - 3
 - 0
 - 1
 - 2
 - 3
 - 0
 - 1
-

Problem 8.4 (2) *Correct Answers:*

- 8, 20, 11, 12, 19, 12, 24, 6, 11, 24
 - 16, 1, 19, 20, 0, 20, 5, 14, 19, 5
 - past-tense
-

Problem 8.4 (3) *Correct Answers:*

- 23, 15, 18, 12, 4
 - 10, 2, 5, 26, 18
 - jbezr
-

Problem 8.4 (4) *Correct Answers:*

- 20
 - 15
 - 1
 - 4
 - 11
 - 6
 - 19
 - 22
 - 20
 - 15
 - 1
 - 4
 - t
 - o
 - a
 - d
-

Problem 8.4 (5) *Correct Answers:*

- 6
- 15
- 18
- 13

- 20
- 2
- 23
- 15
- 6
- 15
- 18
- 13
- f
- o
- r
- m
- form

Problem 8.4 (6) *Correct Answers:*

- 15, 7, 4, 3, 19, 10, 20
- 19, 15, 0, 13, 21, 3, 8
- so-much

Problem 8.4 (7) *Correct Answers:*

- 7, 18, 5, 5, 14, 0, 1, 12, 5, 18, 20
- 6, 23, 25, 25, 7, 5, 9, 26, 25, 23, 4
- fwyygeizywd

8.5 Frequency Analysis

Problem 8.5 (1) (1 point)

Let

$$\mathbb{A} = \{-, a, b, c, \dots, z\}$$

where $-$ represents the character space.

Which four characters from $\mathbb{A}$ occur most frequently in English language texts (written in lower case only)?

Most frequently: ____

2nd most frequently: ____

3rd most frequently: ____

4th most frequently: ____

Problem 8.5 (2) (1 point)

We represent the character space by $-$.

The eavesdropper Eve knows that Alice and Bob use a Caesar Cipher in their secure communication. Eve intercepts the following message sent from Alice to Bob:

kzrfygqzyjmrymdyds1

Eve counts the frequency of the characters and concludes that the character space is encrypted as the character ____.

Problem 8.5 (3) (1 point)

We represent the character space by $-$.

The eavesdropper Eve knows that Alice and Bob use a Caesar Cipher in their secure communication. Eve intercepts the following message sent from Alice to Bob:

oekqmzbbqieedqruczjqriqcktyqriqzqdvvuqwhcqoek

Eve counts the frequency of the characters and concludes that the character $-$ (space) was encrypted as the character ____.

This tells Eve which **encryption** function Alice used. Alice's encryption function $E : \mathbb{A} \rightarrow \mathbb{A}$ is given by:

$E(-) =$ ____,

$E(a) =$ ____,

$E(b) =$ ____,

$E(c) =$ ____,

$E(d) =$ ____,

$E(e) =$ ____,

$D(u) = ___,$
 $D(v) = ___,$
 $D(w) = ___,$
 $D(x) = ___,$
 $D(y) = ___,$
 $D(z) = ___,$

Using the function D Eve decrypts the message and obtains:

Problem 8.5 (4) (1 point)

We represent the character space by $\mathbb{A}$.

The eavesdropper Eve knows that Alice and Bob use a Caesar Cipher in their secure communication. Eve intercepts the following message sent from Alice to Bob:

xnawukqwoqnawsawzxjwikrawejwpeiawxj – wolxza

Eve counts the frequency of the characters and concludes that the character $_$ (space) was encrypted as the character $___$.

This tells Eve which **encryption** function Alice used. Alice's encryption function $E : \mathbb{A} \rightarrow \mathbb{A}$ is given by:

$E(_) = ___,$
 $E(a) = ___,$
 $E(b) = ___,$
 $E(c) = ___,$
 $E(d) = ___,$
 $E(e) = ___,$
 $E(f) = ___,$
 $E(g) = ___,$
 $E(h) = ___,$
 $E(i) = ___,$
 $E(j) = ___,$
 $E(k) = ___,$
 $E(l) = ___,$
 $E(m) = ___,$
 $E(n) = ___,$
 $E(o) = ___,$
 $E(p) = ___,$
 $E(q) = ___,$
 $E(r) = ___,$
 $E(s) = ___,$
 $E(t) = ___,$
 $E(u) = ___,$
 $E(v) = ___,$

$E(w) = ______$,
 $E(x) = ______$,
 $E(y) = ______$,
 $E(z) = ______$,

Now Eve also knows the **decryption** function $D : \mathbb{A} \rightarrow \mathbb{A}$. Recall that the input for the decryption function is the cipher text, and the output of the decryption function is the plain text. The decryption function D is given by:

$D(-) = ______$,
 $D(a) = ______$,
 $D(b) = ______$,
 $D(c) = ______$,
 $D(d) = ______$,
 $D(e) = ______$,
 $D(f) = ______$,
 $D(g) = ______$,
 $D(h) = ______$,
 $D(i) = ______$,
 $D(j) = ______$,
 $D(k) = ______$,
 $D(l) = ______$,
 $D(m) = ______$,
 $D(n) = ______$,
 $D(o) = ______$,
 $D(p) = ______$,
 $D(q) = ______$,
 $D(r) = ______$,
 $D(s) = ______$,
 $D(t) = ______$,
 $D(u) = ______$,
 $D(v) = ______$,
 $D(w) = ______$,
 $D(x) = ______$,
 $D(y) = ______$,
 $D(z) = ______$,

Using the function D Eve decrypts the message and obtains:

Problem 8.5 (5) (1 point)

We represent the character space by $\mathbb{A}$.

The eavesdropper Eve knows that Alice and Bob use a Caesar Cipher in their secure communication. Eve intercepts the following message sent from Alice to Bob:

zrqxeltxyzlrqxrmykaxaltk

Eve counts the frequency of the characters and concludes that the character has to be decrypted as the character (space).

With this Eve finds the **decryption** function $D : \mathbb{A} \rightarrow \mathbb{A}$. Recall that the input for the decryption function is the cipher text, and the output of the decryption function is the plain text. The decryption function D is given by:

$D(-) = ___,$
 $D(a) = ___,$
 $D(b) = ___,$
 $D(c) = ___,$
 $D(d) = ___,$
 $D(e) = ___,$
 $D(f) = ___,$
 $D(g) = ___,$
 $D(h) = ___,$
 $D(i) = ___,$
 $D(j) = ___,$
 $D(k) = ___,$
 $D(l) = ___,$
 $D(m) = ___,$
 $D(n) = ___,$
 $D(o) = ___,$
 $D(p) = ___,$
 $D(q) = ___,$
 $D(r) = ___,$
 $D(s) = ___,$
 $D(t) = ___,$
 $D(u) = ___,$
 $D(v) = ___,$
 $D(w) = ___,$
 $D(x) = ___,$
 $D(y) = ___,$
 $D(z) = ___,$

Using the function D Eve decrypts the message and obtains:

Problem 8.5 (6) (1 point)

We represent the character space by .

The eavesdropper Eve knows that Alice and Bob use a Caesar Cipher in their secure communication. Eve intercepts the following message sent from Alice to Bob:

rdoqhvrqbseuoqckijqyrlvqvnjvdizedqzdqwekhquzhvtjzedi

Eve counts the frequency of the characters and concludes that the character space is encrypted as the character ____.

With this information Eve decrypts the message and obtains:

Problem 8.5 (7) (1 point)

We represent the character space by Σ .

The eavesdropper Eve knows that Alice and Bob use a Caesar Cipher in their secure communication. Eve intercepts the following message sent from Alice to Bob:

tjpvywivhj Σ vdivodh Σ

Eve counts the frequency of the characters and concludes that the character space is encrypted as the character ____.

With this information Eve decrypts the message and obtains:

Problem 8.5 (8) (1 point)

Find the quotients and remainders:

$84411 \div 2821 = \underline{\hspace{1cm}}$ and

$84411 \bmod 2821 = \underline{\hspace{1cm}}$

$-55426 \div 2371 = \underline{\hspace{1cm}}$ and

$-55426 \bmod 2371 = \underline{\hspace{1cm}}$

$-91199 \div 213 = \underline{\hspace{1cm}}$ and

$-91199 \bmod 213 = \underline{\hspace{1cm}}$

$-28711 \div 2717 = \underline{\hspace{1cm}}$ and

$-28711 \bmod 2717 = \underline{\hspace{1cm}}$

Solutions

Problem 8.5 (1) *Correct Answers:*

- -
 - e
 - t
 - a
-

Problem 8.5 (2) *Correct Answers:*

- y
-

Problem 8.5 (3) *Correct Answers:*

- q
- q
- r
- s
- t
- u
- v
- w
- x
- y
- z
- -
- a
- b
- c
- d
- e
- f
- g
- h
- i
- j
- k
- l
- m
- n
- o
- p
- j
- k
- l
- m
- n
- o
- p

- q
- r
- s
- t
- u
- v
- w
- x
- y
- z
- -
- a
- b
- c
- d
- e
- f
- g
- h
- i
- you-will-soon-admit-as-much-as-i-need-from-you

Problem 8.5 (4) *Correct Answers:*

- w
- w
- x
- y
- z
- -
- a
- b
- c
- d
- e
- f
- g
- h
- i
- j
- k
- l
- m
- n
- o
- p
- q
- r

- s
- t
- u
- v
- d
- e
- f
- g
- h
- i
- j
- k
- l
- m
- n
- o
- p
- q
- r
- s
- t
- u
- v
- w
- x
- y
- z
- -
- a
- b
- c
- are-you-sure-we-can-move-in-time-and-space

Problem 8.5 (5) *Correct Answers:*

- x
- c
- d
- e
- f
- g
- h
- i
- j
- k
- l
- m
- n

- o
- p
- q
- r
- s
- t
- u
- v
- w
- x
- y
- z
- -
- a
- b
- but-how-about-up-and-down

Problem 8.5 (6) *Correct Answers:*

- q
- any-real-body-must-have-extension-in-four-directions

Problem 8.5 (7) *Correct Answers:*

- v
- you-can-move-in-time

Problem 8.5 (8) *Correct Answers:*

- 29
- 2602
- -24
- 1478
- -429
- 178
- -11
- 1176

Chapter 9

Cardinality

1. Definition of Cardinality
2. Infinite Sets
3. Cardinality of Cartesian Products
4. Number of Subsets

9.1 Definition of Cardinality

Problem 9.1 (1) (1 point)

Complete the following:

Let A and B be nonempty sets.

We say that A and B have the same (A) if there exists (B) function $f : A \rightarrow B$.

(A): [select: | **cardinality** | **depth** | **height** | **volume** | **width**]

(B): [select: | **a good** | **an injective** | **an invertible** | **a nice** | **an onto**]

We say that the (C) of A is n if there is (D) function from A to (E).

(C): [select: | **cardinality** | **depth** | **height** | **volume** | **width**]

(D): [select: | **a good** | **an injective** | **an invertible** | **a nice** | **an onto**]

(E): [select: | **the set of natural numbers** | **the set of integers** | $\{0, 1, 2, \dots, n-1\}$ | $\{0, 1, 2, \dots, n\}$ | $\{n\}$ | $\{-n, -n+1, -n+2, \dots, 1\}$]

If such a function exists we call A finite. If A is finite we denote the _____ of A by $\#A$.

[select: | **cardinality** | **depth** | **height** | **volume** | **width**]

Problem 9.1 (2) (1 point)

Let $f : \mathbb{Z}_3 \rightarrow \mathbb{Z}_3$, $f(x) = (2+x) \bmod 3$.

Evaluate f at all elements of the domain:

$f(0) = \underline{\hspace{2cm}}$

$f(1) = \underline{\hspace{2cm}}$

$f(2) = \underline{\hspace{2cm}}$

The function f is invertible. Find the image of the inverse f^{-1} of f at all elements of its domain.

$$f^{-1}(0) = \text{---}$$

$$f^{-1}(1) = \text{---}$$

$$f^{-1}(2) = \text{---}$$

Problem 9.1 (3) (1 point)

Let D be a set. Assume there is an invertible function

$$h : D \rightarrow \mathbb{Z}_5$$

Then the cardinality of D is ____.

Problem 9.1 (4) (1 point)

Let X be a set. Assume there is an invertible function

$$g : X \rightarrow \{0, 1, 2, \dots, 7\}.$$

Then the number of elements in X is ____.

Problem 9.1 (5) (1 point)

Let $X = \{-8, -7, -6, \dots, 11\}$.

Because there is an invertible function

$$h : \{0, 1, 2, \dots, \text{---}\} \rightarrow X$$

the number of elements in X is ____.

Problem 9.1 (6) (1 point)

Determine whether the two sets A and B have the same cardinality.

1. ____ $A = \{x \mid x \in \mathbb{N} \text{ and } x \bmod 2 = 0\}$ and $B = \mathbb{N}$
2. ____ $A = \{1, 2, 3, \dots, 25\}$ and $B = \mathbb{Z}_{25}$
3. ____ $A = \{1, 2, 3, \dots, 14\}$ and $B = \mathbb{Z}_{14}$
4. ____ $A = \{\dots, -3, -2, -1\}$ and $B = \mathbb{N}$

Problem 9.1 (7) (1 point)

$$\#\mathbb{Z}_{48}^{\otimes} = \underline{\hspace{2cm}}$$

Problem 9.1 (8) (1 point)

$$\#\mathbb{Z}_{109} = \underline{\hspace{2cm}}$$

Problem 9.1 (9) (1 point)

The cardinality of the set $\{x \mid x \text{ is an integer and } x > 10 \text{ and } x < 23\}$
is $\underline{\hspace{2cm}}$

Problem 9.1 (10) (1 point)

$$\#\{\} = \underline{\hspace{2cm}}$$

Problem 9.1 (11) (1 point)

$$\#\{\} = \underline{\hspace{2cm}}$$

$$\#\{0\} = \underline{\hspace{2cm}}$$

$$\#\{-30, -29, -28\} = \underline{\hspace{2cm}}$$

Problem 9.1 (12) (1 point)

The cardinality of the set $\{43, 44, 45, \dots, 127\}$ is: $\underline{\hspace{2cm}}$

Solutions

Problem 9.1 (1) *Correct Answers:*

- cardinality
- an invertible
- cardinality
- an invertible
- $\{0, 1, 2, \dots, n-1\}$
- cardinality

Problem 9.1 (2) *Correct Answers:*

- 2
- 0
- 1
- 1
- 2
- 0

Problem 9.1 (3) *Correct Answers:*

- 5

Problem 9.1 (4) *Correct Answers:*

- 8

Problem 9.1 (5) *Correct Answers:*

- 19
- 20

Problem 9.1 (6) *Correct Answers:*

- I
- I
- I
- I

Problem 9.1 (7) *Correct Answers:*

- 47

Problem 9.1 (8) *Correct Answers:*

- 109

Problem 9.1 (9) *Correct Answers:*

- 12

Problem 9.1 (10) *Correct Answers:*

- 0

Problem 9.1 (11) *Correct Answers:*

- 0
- 1
- 3

Problem 9.1 (12) *Correct Answers:*

- 85

Problem 9.2 (3) (1 point)

Determine whether the two sets have the same cardinality.

1. ___ $\{1, 2, 3, \dots, 2324\}$ and $\mathbb{N}$
2. ___ The set of even natural numbers and $\mathbb{N}$
3. ___ The set of odd natural numbers and $\mathbb{N}$
4. ___ $\mathbb{Z}$ and $\mathbb{N}$

Problem 9.2 (4) (1 point)

Complete the following:

Let A and B be nonempty sets.

We say that A and B have the same $\text{---}^{(A)}\text{---}$ if there exists $\text{---}^{(B)}\text{---}$ function $f : A \rightarrow B$.

(A): [select: | **cardinality** | **depth** | **height** | **volume** | **width**]

(B): [select: | **a good** | **an injective** | **an invertible** | **a nice** | **an onto**]

We say that A is $\text{---}^{(C)}\text{---}$ if there is $\text{---}^{(D)}\text{---}$ function from A to the set of natural numbers.

(C): [select: | **accountable** | **countable** | **innocent** | **numbered** | **unaccountable** | **uncountable**]

(D): [select: | **a good** | **an injective** | **an invertible** | **a nice** | **an onto**]

Problem 9.2 (5) (1 point)

For each of these sets decide whether it is finite, infinite and countable or infinite and not countable.

Select the correct statement:

1. ___ $\{-7, -6, -5, \dots, 1\}$
2. ___ $\{x \mid x \in \mathbb{N} \text{ and } x \leq 16 \text{ and } x \bmod 2 = 0\}$
3. ___ $\{x \mid x \in \mathbb{N} \text{ and } x \bmod 2 = 0\}$
4. ___ the set of negative integers

Problem 9.2 (6) (1 point)

For each of these sets decide whether it is finite, infinite and countable or infinite and not countable.

Select the correct statement:

1. ☐ $\{7\}$
2. ☐ $\mathbb{Z}_{16}^{\otimes}$
3. ☐ $\{-15, -14, -13, \dots, 7\}$
4. ☐ $\{x \mid x \in \mathbb{N} \text{ and } x \leq 8 \text{ and } x \bmod 2 = 0\}$

Solutions

Problem 9.2 (1) *Correct Answers:*

- cardinality
 - an invertible
 - finite
 - an invertible
 - $\{0, 1, 2, \dots, n-1\}$
 - infinite
-

Problem 9.2 (2) *Correct Answers:*

- A
 - B
 - C
-

Problem 9.2 (3) *Correct Answers:*

- Not
 - Same
 - Same
 - Same
-

Problem 9.2 (4) *Correct Answers:*

- cardinality
 - an invertible
 - countable
 - an invertible
-

Problem 9.2 (5) *Correct Answers:*

- F
 - F
 - C
 - C
-

Problem 9.2 (6) *Correct Answers:*

- F
- F
- F
- F

9.3 Cardinality of Cartesian Products

Problem 9.3 (1) (1 point)

Let $A = \{3, 4, 5\}$ and let $B = \{-2, -1\}$. Give the set in roster form.

$A \times B = \{\text{_____}\}$

Problem 9.3 (2) (1 point)

Complete the following:

Let A and B be sets.

The ^(A) of the sets A and B , denoted by $A \times B$, is the set of all ^(B) (a, b) where a is ^(C) the set A ^(D) b is ^(E) the set B .

(A): [select: | **intersection** | **union** | **difference** | **sum** | **Cartesian product** | **complement**]

(B): [select: | **unordered pairs** | **ordered pairs** | **sets** | **numbers**]

(C): [select: | **related to** | **an element of** | **a subsets of** | **not related to** | **not an element of** | **a proper subset of** | **equal to** | **not equal to**]

(D): [select: | **and** | **or**]

(E): [select: | **related to** | **an element of** | **a subsets of** | **not related to** | **not an element of** | **a proper subset of** | **equal to** | **not equal to**]

The ^(F) of the ^(G) of A and B is $\#A \cdot \#B$.

(F): [select: | **weight** | **volume** | **size** | **length** | **area** | **cardinality**]

(G): [select: | **intersection** | **union** | **difference** | **sum** | **Cartesian product** | **complement**]

Problem 9.3 (3) (1 point)

Let $A = \{1, 2, 3, \dots, 6\}$ and $B = \{1, 2, 3, \dots, 10\}$.

The number of elements in A is ____.

The number of elements in B is ____.

The number of elements in $A \times B$ is ____.

Problem 9.3 (4) (1 point)

What is the number of elements in $\mathbb{Z}_5 \times \mathbb{Z}_8$? ____

Problem 9.3 (5) (1 point)

Let $A = \{4, 5, 6, \dots, 15\}$ and $B = \{4, 5, 6, \dots, 18\}$.

What is the number of elements in $A \times B$? ____

Problem 9.3 (6) (1 point)

Let $A = \{a, b, c\}$, $B = \{1, 2, 3\}$

How many elements are in $A \times B$? ____

Give $A \times B$ in roster form.

$A \times B = \{\text{_____}\}$

[Note: Enter your answer as a comma-separated list. Pairs should be denoted with parentheses.]

Problem 9.3 (7) (1 point)

Alice and Bob are playing a game of Go on a 11×11 board. Alice is the first to set a stone on the empty board. The rules of Go allow her to place the stone on any of the fields of the board. How many different choices does she have for her first move ? ____

Solutions

Problem 9.3 (1) *Correct Answers:*

- $(3, -2), (3, -1), (4, -2), (4, -1), (5, -2), (5, -1)$
-

Problem 9.3 (2) *Correct Answers:*

- Cartesian product
 - ordered pairs
 - an element of
 - and
 - an element of
 - cardinality
 - Cartesian product
-

Problem 9.3 (3) *Correct Answers:*

- 6
 - 10
 - 60
-

Problem 9.3 (4) *Correct Answers:*

- 40
-

Problem 9.3 (5) *Correct Answers:*

- 180
-

Problem 9.3 (6) *Correct Answers:*

Solution:

$$A = \{a, b, c\}$$

$$B = \{1, 2, 3\}$$

The number of elements in a Cartesian product is simply $N(A) \cdot N(B)$ for any sets A, B .

Thus, the number of elements in $A \times B$ is

$$N(A) \cdot N(B) = 3 \cdot 3 = 9$$

The Cartesian product $A \times B$ is defined as the set of all ordered pairs whose first component is a member of A and whose second component is a member of B .

More formally, $A \times B = \{(a, b) | a \in A \text{ and } b \in B\}$

Thus, $A \times B$ is

$$\{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3), (c, 1), (c, 2), (c, 3)\}$$

- 9
 - $(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3), (c, 1), (c, 2), (c, 3)$
-

Problem 9.3 (7) *Correct Answers:*

- 121

9.4 Number of Subsets

Problem 9.4 (1) (1 point)

Let $E = \{a, b, c, f, g\}$.

For each statement indicate whether it is true or false.

1. ☐ $\{d\} \subseteq E$
2. ☐ $\{a, b, d\} \subseteq E$
3. ☐ $\{f, g\} \not\subseteq E$
4. ☐ $\{c\} \subseteq E$

Problem 9.4 (2) (1 point)

Let $A = \{a_1, a_2, a_3, \dots, a_n\}$.

Let N be the number of distinct subsets of A .

Let b be an element not contained in A .

Let $B = \{a_1, a_2, a_3, \dots, a_n, b\}$, that is, B contains all elements of A and the additional element b .

What is the number of distinct subsets of B ?

- A. $2 \cdot N$
- B. $N + 1$
- C. N^2
- D. N
- E. $N + 2$
- F. $N - 1$
- G. $N - 2$
- H. $N/2$

Problem 9.4 (3) (1 point)

Let A be a set and let n be the cardinality of A .

What is the number of distinct subsets of A ?

- A. $2 \cdot n$
- B. 2^n

- C. $n + 2$
- D. $n - 1$
- E. $n + 1$
- F. n
- G. $n - 2$
- H. n^2
- I. $n/2$

Problem 9.4 (4) (1 point)

Let $S = \{6, 7, 8, \dots, 15\}$.

The cardinality of S is: ____

Thus the number of distinct subsets of $\{6, 7, 8, \dots, 15\}$ is: ____

Problem 9.4 (5) (1 point)

The number of distinct subsets of $6, 7, 8, \dots, 25$ is: _____

Problem 9.4 (6) (1 point)

The number of distinct subsets of $\mathbb{Z}_6$ is: _____

Problem 9.4 (7) (1 point)

The number of distinct subsets of $\mathbb{Z}_7^\otimes$ is: _____

Problem 9.4 (8) (1 point)

The Friendly Bike Store offers the options kickstand, umbrella holder for handle bar, hub dynamo, hydraulic breaks, rack (front), rack (back), and bell on its bikes.

Customers can choose between _____ different combinations of options.

Problem 9.4 (9) (1 point)

At Sandwich Shack you can order sandwiches with lettuce, peppers, spinach, feta, salami, and pickles. How many different combinations of sandwiches can a customer choose ? _____

Solutions

Problem 9.4 (1) *Correct Answers:*

Solution:

$$E = \{a, b, c, f, g\}$$

Subsets of E include:

$$\{a, f, g\}$$

$$\{a, b, c, f, g\}$$

Remember that a set is always a subset of itself. By definition, for sets A and B , $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$. From this definition, it is clear that since $A = A$ for any set A , $A \subseteq A$ must also be true.

Correct Answers:

- F
- F
- F
- T

Problem 9.4 (2) *Correct Answers:*

- A

Problem 9.4 (3) *Correct Answers:*

- B

Problem 9.4 (4) *Correct Answers:*

- 10
- 1024

Problem 9.4 (5) *Correct Answers:*

- 1048576

Problem 9.4 (6) *Correct Answers:*

- 64

Problem 9.4 (7) *Correct Answers:*

- 64

Problem 9.4 (8) *Correct Answers:*

- 128

Problem 9.4 (9) *Correct Answers:*

- 64

Chapter 10

Primes

1. Definition of a Prime
2. Sieve of Eratosthenes
3. Prime Factorization
4. Infinitude of Primes
5. Twin Prime Conjecture

10.1 Definition of a Prime

Problem 10.1 (1) (1 point)

Let n be a natural number greater than 1. If n and 1 are the only positive factors of n , then (select all statements that are true):

- A. n is prime.
 - B. n is not composite
 - C. n is composite.
 - D. n is not prime.
 - E. n has a positive factor a with $a \neq 1$ and $a \neq n$
-

Problem 10.1 (2) (1 point)

Let n be a natural number. If there are natural numbers a and b with $a \neq 1$ and $b \neq 1$ such that $n = a \cdot b$, then (select all statements that are true):

- A. n is prime.
 - B. n is composite.
 - C. The positive factors of n include 1, a , b and n .
 - D. n is not composite
 - E. n is not prime.
 - F. The only positive factors of n are 1 and n .
-

Problem 10.1 (3) (1 point)

A number with exactly two distinct divisors (namely 1 and itself) is called *prime*.

A number with more than two (distinct) positive divisors is called *composite*.

The smallest number that is a prime is ____.

The smallest number that is composite is ____.

There are ____ primes that are less than 10.

There are ____ composites that are less than 10.

The smallest prime greater than 50 is ____

Problem 10.1 (4) (1 point)

Compute the remainder and complete the statement about divisibility

Because $52 \bmod 13 = \underline{\hspace{1cm}}$,
we have that $13 \underline{\hspace{1cm}} 52$. [select: | **divides** | **does not divide**]

Because $42 \bmod 18 = \underline{\hspace{1cm}}$,
we have that $18 \underline{\hspace{1cm}} 42$. [select: | **divides** | **does not divide**]

Because $8 \bmod 18 = \underline{\hspace{1cm}}$,
we have that $18 \underline{\hspace{1cm}} 8$. [select: | **divides** | **does not divide**]

Because $6 \bmod 20 = \underline{\hspace{1cm}}$,
we have that $20 \underline{\hspace{1cm}} 6$. [select: | **divides** | **does not divide**]

Because $6 \bmod 3 = \underline{\hspace{1cm}}$,
we have that $3 \underline{\hspace{1cm}} 6$. [select: | **divides** | **does not divide**]

Because $25 \bmod 20 = \underline{\hspace{1cm}}$,
we have that $20 \underline{\hspace{1cm}} 25$. [select: | **divides** | **does not divide**]

Solutions

Problem 10.1 (1) *Correct Answers:*

- AB
-

Problem 10.1 (2) *Correct Answers:*

- BCE
-

Problem 10.1 (3) *Correct Answers:*

Solution:

1 is not a prime, nor is it composite, it is called a unit. 2 is a prime so it is the smallest prime. 3 is a prime. 4 is a composite so it is the smallest composite.

The primes less than 10 are 2,3,5,7, so there are 4 of them. The composites less than 10 are 4,6,8,9 so there are 4 of them

Since $51 = 17 \times 3$, $52 = 2^2 \times 13$, and 53 is prime so it is the smallest prime greater than 50.

Correct Answers:

- 2
 - 4
 - 4
 - 4
 - 53
-

Problem 10.1 (4) *Correct Answers:*

- 0
- divides
- 6
- does not divide
- 8
- does not divide
- 6
- does not divide
- 0
- divides
- 5
- does not divide

10.2 Sieve of Eratosthenes

Problem 10.2 (1) (1 point)

In this problem you are asked to go through the first steps of the Sieve of Eratosthenes for the integers from 2220 to 2244.

Hint: 2220 is divisible by 2,3, and 5.

Check all numbers that are multiples of 2, 3, or 5.

- A. 2220
- B. 2221
- C. 2222
- D. 2223
- E. 2224
- F. 2225
- G. 2226
- H. 2227
- I. 2228
- J. 2229
- K. 2230
- L. 2231
- M. 2232
- N. 2233
- O. 2234
- P. 2235
- Q. 2236
- R. 2237
- S. 2238
- T. 2239
- U. 2240
- V. 2241
- W. 2242
- X. 2243
- Y. 2244

Problem 10.2 (2) (1 point)

Use the Sieve of Eratosthenes to check all composite numbers up to 31.

- A. 2
- B. 3
- C. 4
- D. 5
- E. 6
- F. 7

- G. 8
- H. 9
- I. 10
- J. 11
- K. 12
- L. 13
- M. 14
- N. 15
- O. 16
- P. 17
- Q. 18
- R. 19
- S. 20
- T. 21
- U. 22
- V. 23
- W. 24
- X. 25
- Y. 26
- Z. 27
- AA. 28
- AB. 29
- AC. 30
- AD. 31

Now the unchecked numbers are the prime numbers.

Thus the prime numbers up to 31 are: [give a comma separated list of numbers, e.g: 2,3,5]

Problem 10.2 (3) (1 point)

The number of primes from 0 to 30 is ____

The number of primes from 30 to 60 is ____

The number of primes from 60 to 90 is ____

The number of primes from 90 to 120 is ____

The number of primes from 120 to 150 is ____

The number of primes from 150 to 180 is ____

The number of primes from 180 to 210 is ____

Problem 10.2 (4) (1 point)

For each of the following numbers write down the list of prime numbers less or equal to the given number in increasing order separated by commas.

For example, the prime numbers less than or equal to 7 in increasing order are 2, 3, 5, 7.

The prime numbers less than or equal to 20 in increasing order are

The prime numbers less than or equal to 38 in increasing order are

The prime numbers less than or equal to 67 in increasing order are

The prime numbers less than or equal to 80 in increasing order are

Problem 10.2 (5) (1 point)

Let a be an integer.

Suppose that the remainder when a is divided by 3 is 2 and the remainder when b is divided by 3 is 0.

That is, $a \bmod 3 = 2$ and $b \bmod 3 = 0$.

Find:

$$(a + a) \bmod 3 = \underline{\hspace{1cm}}$$

$$(a + b) \bmod 3 = \underline{\hspace{1cm}}$$

$$(a \cdot b) \bmod 3 = \underline{\hspace{1cm}}$$

$$(a + 2) \bmod 3 = \underline{\hspace{1cm}}$$

$$(2 \cdot b) \bmod 3 = \underline{\hspace{1cm}}$$

Solutions

Problem 10.2 (1) *Correct Answers:*

- ACDEFGHIJKMOPQSUVWY
-

Problem 10.2 (2) *Correct Answers:*

- CEGHIKMNOQSTUWXYZAAAC
 - 2,3,5,7,11,13,17,19,23,29,31
-

Problem 10.2 (3) *Correct Answers:*

- 10
 - 7
 - 7
 - 6
 - 5
 - 6
 - 5
-

Problem 10.2 (4) *Correct Answers:*

- 2,3,5,7,11,13,17,19
 - 2,3,5,7,11,13,17,19,23,29,31,37
 - 2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67
 - 2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79
-

Problem 10.2 (5) *Correct Answers:*

- 1
- 2
- 0
- 1
- 0

10.3 Prime Factorization

Problem 10.3 (1) (1 point)

We call all primes numbers that divide a number, the prime divisors of the number.

For each of the following numbers write down the number's prime divisors as a comma-separated list (so, "5" or "2,3" for 25 and 12 respectively, but without the quotes).

The prime divisors of 86 are _____

The prime divisors of 39 are _____

The prime divisors of 21 are _____

The prime divisors of 132 are _____

Problem 10.3 (2) (1 point)

For $n = 30$, find the prime factorization.

[Note: Enter your answer as a comma-separated list. If the factorization is $2^2 \cdot 3^2$, enter your answer as 2,2,3,3]

Problem 10.3 (3) (1 point)

We have $1400 = 2 \cdot 2 \cdot 2 \cdot 5 \cdot 5 \cdot 7$.

Which expression is equal to 1400

- A. $2^3 \cdot 5^2 \cdot 7^0$
- B. $2^3 \cdot 5^2 \cdot 7^1$
- C. $2^2 \cdot 5^1 \cdot 7^1$
- D. $2^2 \cdot 5^1 \cdot 7^0$

Problem 10.3 (4) (1 point)

What are the greatest common divisors of the following pairs of integers ?

If $a = 2^3 \cdot 3 \cdot 5^3$ and $b = 2^3 \cdot 3^5 \cdot 5^5$ then
 $\gcd(a, b) =$ _____

If $a = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$ and $b = 2^2 \cdot 3^5 \cdot 7^3 \cdot 17$ then
 $\gcd(a, b) =$ _____

If $a = 2^3 \cdot 7$ and $b = 5 \cdot 13$ then
 $\gcd(a, b) = \underline{\hspace{2cm}}$

Problem 10.3 (5) (1 point)

Compute the remainder and complete the statement about divisibility

Because $69 \bmod 16 = \underline{\hspace{1cm}}$,
we have that $16 \underline{\hspace{1cm}} 69$. [select: | **divides** | **does not divide**]

Because $44 \bmod 11 = \underline{\hspace{1cm}}$,
we have that $11 \underline{\hspace{1cm}} 44$. [select: | **divides** | **does not divide**]

Because $5 \bmod 20 = \underline{\hspace{1cm}}$,
we have that $20 \underline{\hspace{1cm}} 5$. [select: | **divides** | **does not divide**]

Because $102 \bmod 17 = \underline{\hspace{1cm}}$,
we have that $17 \underline{\hspace{1cm}} 102$. [select: | **divides** | **does not divide**]

Because $75 \bmod 6 = \underline{\hspace{1cm}}$,
we have that $6 \underline{\hspace{1cm}} 75$. [select: | **divides** | **does not divide**]

Because $2 \bmod 7 = \underline{\hspace{1cm}}$,
we have that $7 \underline{\hspace{1cm}} 2$. [select: | **divides** | **does not divide**]

Problem 10.3 (6) (1 point)

We want to determine whether the integer 527 is prime or composite.

Let w be an approximation to the square root of 527 (to a precision of at least one digit after the decimal point).

We use $w = \underline{\hspace{1cm}}$ (give at least one digit after the decimal point).

In the following select ‘we do not need to check divisibility’, if the selection for a previous line already allows you to make a conclusion about the primality of 527.

2 is $\underline{\hspace{1cm}}$ ^(A) and $\underline{\hspace{1cm}}$ ^(B).

(A): [select: | **less than w** | **greater than w**]

(B): [select: | **divides 527** | **does not divide 527** | **we do not need to check divisibility**]

3 is (A) and (B) .

(A): [select: | **less than w** | **greater than w**]

(B): [select: | **divides 527** | **does not divide 527** | **we do not need to check divisibility**]

5 is (A) and (B) .

(A): [select: | **less than w** | **greater than w**]

(B): [select: | **divides 527** | **does not divide 527** | **we do not need to check divisibility**]

7 is (A) and (B) .

(A): [select: | **less than w** | **greater than w**]

(B): [select: | **divides 527** | **does not divide 527** | **we do not need to check divisibility**]

11 is (A) and (B) .

(A): [select: | **less than w** | **greater than w**]

(B): [select: | **divides 527** | **does not divide 527** | **we do not need to check divisibility**]

13 is (A) and (B) .

(A): [select: | **less than w** | **greater than w**]

(B): [select: | **divides 527** | **does not divide 527** | **we do not need to check divisibility**]

17 is (A) and (B) .

(A): [select: | **less than w** | **greater than w**]

(B): [select: | **divides 527** | **does not divide 527** | **we do not need to check divisibility**]

19 is (A) and (B) .

(A): [select: | **less than w** | **greater than w**]

(B): [select: | **divides 527** | **does not divide 527** | **we do not need to check divisibility**]

23 is (A) and (B) .

(A): [select: | **less than w** | **greater than w**]

(B): [select: | **divides 527** | **does not divide 527** | **we do not need to check divisibility**]

29 is (A) and (B) .

(A): [select: | **less than w** | **greater than w**]

(B): [select: | **divides 527** | **does not divide 527** | **we do not need to check divisibility**]

31 is (A) and (B) .

(A): [select: | **less than w** | **greater than w**]

(B): [select: | **divides 527** | **does not divide 527** | **we do not need to check divisibility**]

Now conclude whether 527 is prime or composite. The integer 527 is _____ [select: | **prime** | **composite**]

Problem 10.3 (7) (1 point)

We want to determine whether the integer 299 is prime or composite.

Let w be an approximation to the square root of 299 (to a precision of at least one digit after the decimal point).

We use $w = \underline{\hspace{1cm}}$ (give at least one digit after the decimal point).

In the following select 'we do not need to check divisibility', if the selection for a previous line already allows you to make a conclusion about the primality of 299.

2 is $\underline{\hspace{1cm}}^{(A)}$ and $\underline{\hspace{1cm}}^{(B)}$.

(A): [select: | **less than w** | **greater than w**]

(B): [select: | **divides 299** | **does not divide 299** | **we do not need to check divisibility**]

3 is $\underline{\hspace{1cm}}^{(A)}$ and $\underline{\hspace{1cm}}^{(B)}$.

(A): [select: | **less than w** | **greater than w**]

(B): [select: | **divides 299** | **does not divide 299** | **we do not need to check divisibility**]

5 is $\underline{\hspace{1cm}}^{(A)}$ and $\underline{\hspace{1cm}}^{(B)}$.

(A): [select: | **less than w** | **greater than w**]

(B): [select: | **divides 299** | **does not divide 299** | **we do not need to check divisibility**]

7 is $\underline{\hspace{1cm}}^{(A)}$ and $\underline{\hspace{1cm}}^{(B)}$.

(A): [select: | **less than w** | **greater than w**]

(B): [select: | **divides 299** | **does not divide 299** | **we do not need to check divisibility**]

11 is $\underline{\hspace{1cm}}^{(A)}$ and $\underline{\hspace{1cm}}^{(B)}$.

(A): [select: | **less than w** | **greater than w**]

(B): [select: | **divides 299** | **does not divide 299** | **we do not need to check divisibility**]

13 is (A) and (B) .

(A): [select: | **less than w** | **greater than w**]

(B): [select: | **divides 299** | **does not divide 299** | **we do not need to check divisibility**]

17 is (A) and (B) .

(A): [select: | **less than w** | **greater than w**]

(B): [select: | **divides 299** | **does not divide 299** | **we do not need to check divisibility**]

19 is (A) and (B) .

(A): [select: | **less than w** | **greater than w**]

(B): [select: | **divides 299** | **does not divide 299** | **we do not need to check divisibility**]

23 is (A) and (B) .

(A): [select: | **less than w** | **greater than w**]

(B): [select: | **divides 299** | **does not divide 299** | **we do not need to check divisibility**]

29 is (A) and (B) .

(A): [select: | **less than w** | **greater than w**]

(B): [select: | **divides 299** | **does not divide 299** | **we do not need to check divisibility**]

31 is (A) and (B) .

(A): [select: | **less than w** | **greater than w**]

(B): [select: | **divides 299** | **does not divide 299** | **we do not need to check divisibility**]

Now conclude whether 299 is prime or composite.

The integer 299 is _____ [select: | **prime** | **composite**]

Solutions

Problem 10.3 (1) *Correct Answers:*

- 2, 43
- 3, 13
- 3, 7
- 2, 3, 11

Problem 10.3 (2) *Correct Answers:*

Solution:

$$n = 30$$

30 has the prime factorization

$$2 \cdot 3 \cdot 5$$

Correct Answers:

- 2, 3, 5

Problem 10.3 (3) *Correct Answers:*

Solution:

Since 2 occurs as a factor in 1400 three times, the expression begins 2^3 .

Since 5 occurs as a factor in 1400 twice, the expression continues 5^2 .

Since 7 occurs as a factor in 1400 once, the expression begins 7^1 .

Since p^0 (which is 1) means that prime p is not a factor of the number, it would make no sense to put p^0 into such an expression because there are infinitely many primes that do not occur in the factorization of any particular number.

Correct Answers:

- B

Problem 10.3 (4) *Correct Answers:*

- 3000
- 84
- 1

Problem 10.3 (5) *Correct Answers:*

- 5
- does not divide
- 0
- divides

- 5
- does not divide
- 0
- divides
- 3
- does not divide
- 2
- does not divide

Problem 10.3 (6) *Correct Answers:*

- 22.956480566498
- less than w
- does not divide 527
- less than w
- does not divide 527
- less than w
- does not divide 527
- less than w
- does not divide 527
- less than w
- does not divide 527
- less than w
- does not divide 527
- less than w
- divides 527
- less than w
- we do not need to check divisibility
- greater than w
- we do not need to check divisibility
- greater than w
- we do not need to check divisibility
- greater than w
- we do not need to check divisibility
- composite

Problem 10.3 (7) *Correct Answers:*

- 17.2916164657906
- less than w
- does not divide 299
- less than w
- does not divide 299
- less than w
- does not divide 299
- less than w
- does not divide 299
- less than w
- does not divide 299

- less than w
- divides 299
- less than w
- we do not need to check divisibility
- greater than w
- we do not need to check divisibility
- greater than w
- we do not need to check divisibility
- greater than w
- we do not need to check divisibility
- greater than w
- we do not need to check divisibility
- composite

10.4 Infinitude of Primes

Problem 10.4 (1) (1 point)

The number of primes from 0 to 40 is ____

The number of primes from 40 to 80 is ____

The number of primes from 80 to 120 is ____

The number of primes from 120 to 160 is ____

The number of primes from 160 to 200 is ____

Problem 10.4 (2) (1 point)

Theorem 1. Let b be a natural number. Then $\gcd(b, b+1) = 1$, that means, b and $b+1$ are coprime.

Theorem 2. Let B be a set. If for each finite subset S of B there is an element $x \in B$ with $x \notin S$, then B is infinite.

We apply the two theorems above in the proof of the next theorem. Fill in the blanks.

Theorem 3. There are infinitely many prime numbers.

Proof. Let $\mathbb{P}$ be the set of _____. [select: | **integers** | **natural numbers** | **prime numbers** | **negative integers**]

Let Q be a _____ of the set $\mathbb{P}$. Denote the elements of Q by $p_1, p_2, \dots, p_n$ and let $q = p_1 \cdot p_2 \cdot \dots \cdot p_n$.
[select: | **finite subset** | **element** | **infinite subset**]

By Theorem 1, q and $q+1$ are _____. [select: | **coprime** | **odd** | **even** | **both prime**]

So there is at least one prime number that $\xrightarrow{(A)} q+1$ but $\xrightarrow{(B)} q$. Let's call this prime number t .

(A): | **is equal to** | **divides** | **does not divide** | **is less than**]

(B): | **is equal to** | **does divide** | **does not divide** | **is greater than**]

Because t does not divide q we have that t is _____ of Q .

[select: | **an element** | **a finite subset** | **not an element** | **a infinite subset**]

So we have shown that for any finite set of prime numbers Q , we can find another prime number that is not in the set Q . Thus, by Theorem 2, we have that $\mathbb{P}$ is _____. [select: | **finite** | **empty** | **not a set** | **infinite**]

Solutions

Problem 10.4 (1) *Correct Answers:*

- 12
- 10
- 8
- 7
- 9

Problem 10.4 (2) *Correct Answers:*

- prime numbers
- finite subset
- coprime
- divides
- does not divide
- not an element
- infinite

10.5 Twin Prime Conjecture

Problem 10.5 (1) (1 point)

Choose the theorem or conjecture that states the following:

According to _____, there are infinitely many primes p such that $p + 2$ is also prime.

[select: | **The Prime Number Theorem** | **The Fundamental Theorem of Arithmetic** | **Fermat's Last Theorem** | **Fermat's Little Theorem** | **Bezout's Identity** | **The Twin Prime Conjecture** | **Goldbach's Conjecture**]

Problem 10.5 (2) (1 point)

The number of primes up to 20 is ____

The number of twin prime pairs up to 20 is ____

The number of primes up to 40 is ____

The number of twin prime pairs up to 40 is ____

The number of primes up to 60 is ____

The number of twin prime pairs up to 60 is ____

The number of primes up to 80 is ____

The number of twin prime pairs up to 80 is ____

Problem 10.5 (3) (1 point)

Decide if each of the following statements is a definition, a theorem or a conjecture.

1. ____ Let $n \in \mathbb{N}$ then $\gcd(n, n + 1) = 1$.
 2. ____ For $n \in \mathbb{N}$ we set $\mathbb{Z}_n^\otimes := \{1, 2, 3, \dots, n - 1\}$.
 3. ____ There are infinitely many prime numbers.
 4. ____ There are infinitely primes p such that $p + 2$ is also a prime number.
-

Problem 10.5 (4) (1 point)

7 is ^(A)____ and is ^(B)____.

(A): [select: | **prime** | **not prime**]

(B): [select: | **in a twin prime pair** | **not in a twin prime pair**]

21 is ^(A) and is ^(B) .

(A): [select: | **prime** | **not prime**]

(B): [select: | **in a twin prime pair** | **not in a twin prime pair**]

39 is ^(A) and is ^(B) .

(A): [select: | **prime** | **not prime**]

(B): [select: | **in a twin prime pair** | **not in a twin prime pair**]

47 is ^(A) and is ^(B) .

(A): [select: | **prime** | **not prime**]

(B): [select: | **in a twin prime pair** | **not in a twin prime pair**]

63 is ^(A) and is ^(B) .

(A): [select: | **prime** | **not prime**]

(B): [select: | **in a twin prime pair** | **not in a twin prime pair**]

77 is ^(A) and is ^(B) .

(A): [select: | **prime** | **not prime**]

(B): [select: | **in a twin prime pair** | **not in a twin prime pair**]

83 is ^(A) and is ^(B) .

(A): [select: | **prime** | **not prime**]

(B): [select: | **in a twin prime pair** | **not in a twin prime pair**]

89 is ^(A) and is ^(B).

(A): [select: | **prime** | **not prime**]

(B): [select: | **in a twin prime pair** | **not in a twin prime pair**]

Problem 10.5 (5) (1 point)

List the twin primes between 1 and 100 as ordered pairs in ascending order.

The twin primes 3 and 5 as an ordered pair are: (3, 5)

Problem 10.5 (6) (1 point)

Determine whether or not the prime is part of a twin prime pair. Enter "1" for a twin prime and "0" otherwise.

___1. 91

___2. 33

___3. 131

___4. 173

___5. 171

___6. 79

Solutions

Problem 10.5 (1) *Correct Answers:*

- The Twin Prime Conjecture

Problem 10.5 (2) *Correct Answers:*

- 8
- 4
- 12
- 5
- 17
- 6
- 22
- 8

Problem 10.5 (3) *Correct Answers:*

- Theorem
- Definition
- Theorem
- Conjecture

Problem 10.5 (4) *Correct Answers:*

- prime
- in a twin prime pair
- not prime
- not in a twin prime pair
- not prime
- not in a twin prime pair
- prime
- not in a twin prime pair
- not prime
- not in a twin prime pair
- not prime
- not in a twin prime pair
- prime
- not in a twin prime pair
- prime
- not in a twin prime pair

Problem 10.5 (5) *Correct Answers:*

- (3, 5)
- (5, 7)
- (11, 13)
- (17, 19)
- (29, 31)

- $(41, 43)$
- $(59, 61)$
- $(71, 73)$

Problem 10.5 (6) *Correct Answers:*

- 0
- 0
- 0
- 0
- 0
- 0

Chapter 11

Other Bases

1. Decimal Representation
2. Binary Representation
3. From Decimal to Binary
4. Base b Numbers
5. From Decimal to Base

11.1 Decimal Representation

Problem 11.1 (1) (1 point)

Give the expanded decimal form of 5092944.

$$\underline{\hspace{1cm}} \cdot 10^6 + \underline{\hspace{1cm}} \cdot 10^5 + \underline{\hspace{1cm}} \cdot 10^4 + \underline{\hspace{1cm}} \cdot 10^3 + \underline{\hspace{1cm}} \cdot 10^2 + \underline{\hspace{1cm}} \cdot 10 + \underline{\hspace{1cm}} \cdot 1$$

Problem 11.1 (2) (1 point)

Give the expanded decimal form of 90884.

$$\underline{\hspace{1cm}} \cdot 10^6 + \underline{\hspace{1cm}} \cdot 10^5 + \underline{\hspace{1cm}} \cdot 10^4 + \underline{\hspace{1cm}} \cdot 10^3 + \underline{\hspace{1cm}} \cdot 10^2 + \underline{\hspace{1cm}} \cdot 10 + \underline{\hspace{1cm}} \cdot 1$$

Problem 11.1 (3) (1 point)

What are the place values of a base 10 number with 5 digits?

leftmost digit $\rightarrow$ $\underline{\hspace{1cm}} \underline{\hspace{1cm}} \underline{\hspace{1cm}} \underline{\hspace{1cm}} \underline{\hspace{1cm}}$ $\leftarrow$ rightmost digit

Problem 11.1 (4) (1 point)

Compute:

$$20838260094400860294 \bmod 10 = \underline{\hspace{2cm}}$$

$$20838260094400860294 \bmod 100 = \underline{\hspace{2cm}}$$

$$20838260094400860294 \bmod 1000 = \underline{\hspace{2cm}}$$

$$20838260094400860294 \bmod 10000 = \underline{\hspace{2cm}}$$

$$20838260094400860294 \bmod 100000 = \underline{\hspace{2cm}}$$

$$20838260094400860294 \bmod 1000000 = \underline{\hspace{2cm}}$$

Solutions

Problem 11.1 (1) *Correct Answers:*

- 5
- 0
- 9
- 2
- 9
- 4
- 4

Problem 11.1 (2) *Correct Answers:*

- 0
- 0
- 9
- 0
- 8
- 8
- 4

Problem 11.1 (3) *Correct Answers:*

- 10000
- 1000
- 100
- 10
- 1

Problem 11.1 (4) *Correct Answers:*

Hint: We have

$$20838260094400860294 \bmod 10 = 4 \bmod 10$$

and

$$20838260094400860294 \bmod 100 = 94 \bmod 100$$

Correct Answers:

- 4
- 94
- 294
- 294
- 60294
- 860294

11.2 Binary Representation

Problem 11.2 (1) (1 point)

Give the expanded base 2 form of 110010_2 .

$$\underline{\hspace{1cm}} \cdot 2^6 + \underline{\hspace{1cm}} \cdot 2^5 + \underline{\hspace{1cm}} \cdot 2^4 + \underline{\hspace{1cm}} \cdot 2^3 + \underline{\hspace{1cm}} \cdot 2^2 + \underline{\hspace{1cm}} \cdot 2 + \underline{\hspace{1cm}} \cdot 1$$

Give 110010_2 in decimal representation.

Problem 11.2 (2) (1 point)

What are the place values of a base 2 number with 5 digits?

leftmost digit $\rightarrow$ $\underline{\hspace{1cm}} \underline{\hspace{1cm}} \underline{\hspace{1cm}} \underline{\hspace{1cm}} \underline{\hspace{1cm}}$ $\leftarrow$ rightmost digit

Convert these base 2 numbers to decimal numbers.

$$0_2 = \underline{\hspace{1cm}} \quad 1_2 = \underline{\hspace{1cm}}$$

$$10_2 = \underline{\hspace{1cm}} \quad 11_2 = \underline{\hspace{1cm}}$$

$$100_2 = \underline{\hspace{1cm}} \quad 101_2 = \underline{\hspace{1cm}} \quad 110_2 = \underline{\hspace{1cm}}$$

$$1000_2 = \underline{\hspace{1cm}} \quad 1001_2 = \underline{\hspace{1cm}} \quad 1010_2 = \underline{\hspace{1cm}} \quad 1110_2 = \underline{\hspace{1cm}}$$

Problem 11.2 (3) (1 point)

Give the expanded base 2 form of 101110_2 .

$$\underline{\hspace{1cm}} \cdot 2^6 + \underline{\hspace{1cm}} \cdot 2^5 + \underline{\hspace{1cm}} \cdot 2^4 + \underline{\hspace{1cm}} \cdot 2^3 + \underline{\hspace{1cm}} \cdot 2^2 + \underline{\hspace{1cm}} \cdot 2 + \underline{\hspace{1cm}} \cdot 1$$

Give 101110_2 in decimal representation.

Problem 11.2 (4) (1 point)

Give the expanded base 2 form of 111101_2 .

$$\underline{\hspace{1cm}} \cdot 2^6 + \underline{\hspace{1cm}} \cdot 2^5 + \underline{\hspace{1cm}} \cdot 2^4 + \underline{\hspace{1cm}} \cdot 2^3 + \underline{\hspace{1cm}} \cdot 2^2 + \underline{\hspace{1cm}} \cdot 2 + \underline{\hspace{1cm}} \cdot 1$$

Give 111101_2 in decimal representation.

Problem 11.2 (5) (1 point)**Count in base 2**

In the first column enter the numbers in base 2. Recall that the characters used to represent base 2 numbers are 0 and 1.

In the other columns enter the values for the digits of the base 2 expansions. For your convenience the last number in each row is the corresponding decimal number.

$$\text{---}_2 = \text{---} \cdot 2^4 + \text{---} \cdot 2^3 + \text{---} \cdot 2^2 + \text{---} \cdot 2^1 + \text{---} \cdot 2^0 = 0$$

$$\text{---}_2 = \text{---} \cdot 2^4 + \text{---} \cdot 2^3 + \text{---} \cdot 2^2 + \text{---} \cdot 2^1 + \text{---} \cdot 2^0 = 1$$

$$\text{---}_2 = \text{---} \cdot 2^4 + \text{---} \cdot 2^3 + \text{---} \cdot 2^2 + \text{---} \cdot 2^1 + \text{---} \cdot 2^0 = 2$$

$$\text{---}_2 = \text{---} \cdot 2^4 + \text{---} \cdot 2^3 + \text{---} \cdot 2^2 + \text{---} \cdot 2^1 + \text{---} \cdot 2^0 = 3$$

$$\text{---}_2 = \text{---} \cdot 2^4 + \text{---} \cdot 2^3 + \text{---} \cdot 2^2 + \text{---} \cdot 2^1 + \text{---} \cdot 2^0 = 4$$

$$\text{---}_2 = \text{---} \cdot 2^4 + \text{---} \cdot 2^3 + \text{---} \cdot 2^2 + \text{---} \cdot 2^1 + \text{---} \cdot 2^0 = 5$$

$$\text{---}_2 = \text{---} \cdot 2^4 + \text{---} \cdot 2^3 + \text{---} \cdot 2^2 + \text{---} \cdot 2^1 + \text{---} \cdot 2^0 = 6$$

$$\text{---}_2 = \text{---} \cdot 2^4 + \text{---} \cdot 2^3 + \text{---} \cdot 2^2 + \text{---} \cdot 2^1 + \text{---} \cdot 2^0 = 7$$

$$\text{---}_2 = \text{---} \cdot 2^4 + \text{---} \cdot 2^3 + \text{---} \cdot 2^2 + \text{---} \cdot 2^1 + \text{---} \cdot 2^0 = 8$$

$$\text{---}_2 = \text{---} \cdot 2^4 + \text{---} \cdot 2^3 + \text{---} \cdot 2^2 + \text{---} \cdot 2^1 + \text{---} \cdot 2^0 = 9$$

$$\text{---}_2 = \text{---} \cdot 2^4 + \text{---} \cdot 2^3 + \text{---} \cdot 2^2 + \text{---} \cdot 2^1 + \text{---} \cdot 2^0 = 10$$

$$\text{---}_2 = \text{---} \cdot 2^4 + \text{---} \cdot 2^3 + \text{---} \cdot 2^2 + \text{---} \cdot 2^1 + \text{---} \cdot 2^0 = 11$$

$$\text{---}_2 = \text{---} \cdot 2^4 + \text{---} \cdot 2^3 + \text{---} \cdot 2^2 + \text{---} \cdot 2^1 + \text{---} \cdot 2^0 = 12$$

$$\text{---}_2 = \text{---} \cdot 2^4 + \text{---} \cdot 2^3 + \text{---} \cdot 2^2 + \text{---} \cdot 2^1 + \text{---} \cdot 2^0 = 13$$

$$\text{---}_2 = \text{---} \cdot 2^4 + \text{---} \cdot 2^3 + \text{---} \cdot 2^2 + \text{---} \cdot 2^1 + \text{---} \cdot 2^0 = 14$$

$$\text{---}_2 = \text{---} \cdot 2^4 + \text{---} \cdot 2^3 + \text{---} \cdot 2^2 + \text{---} \cdot 2^1 + \text{---} \cdot 2^0 = 15$$

$$\text{---}_2 = \text{---} \cdot 2^4 + \text{---} \cdot 2^3 + \text{---} \cdot 2^2 + \text{---} \cdot 2^1 + \text{---} \cdot 2^0 = 16$$

$$\text{---}_2 = \text{---} \cdot 2^4 + \text{---} \cdot 2^3 + \text{---} \cdot 2^2 + \text{---} \cdot 2^1 + \text{---} \cdot 2^0 = 17$$

$$\underline{\hspace{1cm}}_2 = \underline{\hspace{1cm}} \cdot 2^4 + \underline{\hspace{1cm}} \cdot 2^3 + \underline{\hspace{1cm}} \cdot 2^2 + \underline{\hspace{1cm}} \cdot 2^1 + \underline{\hspace{1cm}} \cdot 2^0 = 18$$

$$\underline{\hspace{1cm}}_2 = \underline{\hspace{1cm}} \cdot 2^4 + \underline{\hspace{1cm}} \cdot 2^3 + \underline{\hspace{1cm}} \cdot 2^2 + \underline{\hspace{1cm}} \cdot 2^1 + \underline{\hspace{1cm}} \cdot 2^0 = 19$$

Problem 11.2 (6) (1 point)

Convert these integers from binary to decimal representation:

$$1_2 = \underline{\hspace{2cm}}$$

$$10_2 = \underline{\hspace{2cm}}$$

$$111_2 = \underline{\hspace{2cm}}$$

$$1110_2 = \underline{\hspace{2cm}}$$

$$10000_2 = \underline{\hspace{2cm}}$$

$$100110_2 = \underline{\hspace{2cm}}$$

$$1010011_2 = \underline{\hspace{2cm}}$$

$$11010100_2 = \underline{\hspace{2cm}}$$

Solutions

Problem 11.2 (1) *Correct Answers:*

- 0
 - 1
 - 1
 - 0
 - 0
 - 1
 - 0
 - 50
-

Problem 11.2 (2) *Correct Answers:*

- 16
 - 8
 - 4
 - 2
 - 1
 - 0
 - 1
 - 2
 - 3
 - 4
 - 5
 - 6
 - 8
 - 9
 - 10
 - 14
-

Problem 11.2 (3) *Correct Answers:*

- 0
 - 1
 - 0
 - 1
 - 1
 - 1
 - 0
 - 46
-

Problem 11.2 (4) *Correct Answers:*

- 0
- 1
- 1
- 1
- 1

- 0
- 1
- 61

Problem 11.2 (5) *Correct Answers:*

- 0
- 0
- 0
- 0
- 0
- 0
- 1
- 0
- 0
- 0
- 0
- 1
- 10
- 0
- 0
- 0
- 1
- 0
- 11
- 0
- 0
- 0
- 1
- 1
- 100
- 0
- 0
- 1
- 0
- 0
- 101
- 0
- 0
- 1
- 0
- 1
- 110
- 0
- 0
- 1
- 1
- 0

- 111
- 0
- 0
- 1
- 1
- 1
- 1000
- 0
- 1
- 0
- 0
- 0
- 1001
- 0
- 1
- 0
- 0
- 1
- 1010
- 0
- 1
- 0
- 1
- 0
- 1011
- 0
- 1
- 0
- 1
- 1
- 1100
- 0
- 1
- 1
- 0
- 0
- 1101
- 0
- 1
- 1
- 0
- 1
- 1110
- 0
- 1
- 1
- 1

- 0
- 1111
- 0
- 1
- 1
- 1
- 1
- 10000
- 1
- 0
- 0
- 0
- 0
- 10001
- 1
- 0
- 0
- 0
- 1
- 10010
- 1
- 0
- 0
- 1
- 0
- 10011
- 1
- 0
- 0
- 1
- 1

Problem 11.2 (6) *Correct Answers:*

- 1
- 2
- 7
- 14
- 16
- 38
- 83
- 212

11.3 From Decimal to Binary

Problem 11.3 (1) (1 point)

With the conversion algorithm find the base 2 representation of the decimal number 15.

Input: A base 10 number $a := \underline{\hspace{1cm}}$

Let $q_0 := a$.

Let $r_0 := q_0 \bmod 2 = \underline{\hspace{1cm}}$. Let $q_1 := q_0 \div 2 = \underline{\hspace{1cm}}$.

Let $r_1 := q_1 \bmod 2 = \underline{\hspace{1cm}}$. Let $q_2 := q_1 \div 2 = \underline{\hspace{1cm}}$.

Let $r_2 := q_2 \bmod 2 = \underline{\hspace{1cm}}$. Let $q_3 := q_2 \div 2 = \underline{\hspace{1cm}}$.

Let $r_3 := q_3 \bmod 2 = \underline{\hspace{1cm}}$. Let $q_4 := q_3 \div 2 = \underline{\hspace{1cm}}$.

Output: The expanded base 2 representation of the decimal number 15 is:

$$\begin{aligned} 15 &= r_3 \cdot 2^3 \\ &+ r_2 \cdot 2^2 \\ &+ r_1 \cdot 2^1 \\ &+ r_0 \cdot 2^0 \end{aligned}$$

$$\begin{aligned} &= \underline{\hspace{1cm}} \cdot 2^3 \\ &+ \underline{\hspace{1cm}} \cdot 2^2 \\ &+ \underline{\hspace{1cm}} \cdot 2^1 \\ &+ \underline{\hspace{1cm}} \cdot 2^0 \end{aligned}$$

Now give the base 2 representation of 15.

[Although writing leading zeros is mathematically correct, it will be marked as wrong. Do not put extra zeros in front of your answer. For example, you should write 101 but not 0101.]

$$15 = \underline{\hspace{1cm}}_2$$

Problem 11.3 (2) (1 point)

With the conversion algorithm find the base 2 representation of the decimal number 11.

Input: A base 10 number $a := \underline{\hspace{1cm}}$

Let $q_0 := a$.

Let $r_0 := q_0 \bmod 2 = \underline{\hspace{1cm}}$. Let $q_1 := q_0 \operatorname{div} 2 = \underline{\hspace{1cm}}$.

Let $r_1 := q_1 \bmod 2 = \underline{\hspace{1cm}}$. Let $q_2 := q_1 \operatorname{div} 2 = \underline{\hspace{1cm}}$.

Let $r_2 := q_2 \bmod 2 = \underline{\hspace{1cm}}$. Let $q_3 := q_2 \operatorname{div} 2 = \underline{\hspace{1cm}}$.

Let $r_3 := q_3 \bmod 2 = \underline{\hspace{1cm}}$. Let $q_4 := q_3 \operatorname{div} 2 = \underline{\hspace{1cm}}$.

Output: The expanded base 2 representation of the decimal number 11 is:

$$\begin{aligned} 11 &= r_3 \cdot 2^3 \\ &+ r_2 \cdot 2^2 \\ &+ r_1 \cdot 2^1 \\ &+ r_0 \cdot 2^0 \end{aligned}$$

$$\begin{aligned} &= \underline{\hspace{1cm}} \cdot 2^3 \\ &+ \underline{\hspace{1cm}} \cdot 2^2 \\ &+ \underline{\hspace{1cm}} \cdot 2^1 \\ &+ \underline{\hspace{1cm}} \cdot 2^0 \end{aligned}$$

Now give the base 2 representation of 11.

[Although writing leading zeros is mathematically correct, it will be marked as wrong. Do not put extra zeros in front of your answer. For example, you should write 101 but not 0101.]

$$11 = \underline{\hspace{1cm}}_2$$

Problem 11.3 (3) (1 point)

Convert the following integers from decimal representation to binary (base 2) representation.

[Do not put extra zeros in front of your binary notation or it might confuse WebWorK. So write 101 instead of 0101 etc.]

$$31 = \underline{\hspace{1cm}}_2$$

$$93 = \underline{\hspace{1cm}}_2$$

$$168 = \underline{\hspace{1cm}}_2$$

Problem 11.3 (4) (1 point)

Convert the following integers from decimal representation to binary (base 2) representation.

[Do not put extra zeros in front of your binary notation or it might confuse WebWorK. So write 101 instead of 0101 etc.]

$$46 = \text{_____}_2$$

$$92 = \text{_____}_2$$

$$339 = \text{_____}_2$$

Solutions

Problem 11.3 (1) *Correct Answers:*

- 15
- 1
- 7
- 1
- 3
- 1
- 1
- 1
- 0
- 1
- 1
- 1
- 1
- 1111

Problem 11.3 (2) *Correct Answers:*

- 11
- 1
- 5
- 1
- 2
- 0
- 1
- 1
- 0
- 1
- 0
- 1
- 1
- 1011

Problem 11.3 (3) *Correct Answers:*

- 11111
- 1011101
- 10101000

Problem 11.3 (4) *Correct Answers:*

- 101110
- 1011100
- 101010011

11.4 Base b Numbers

Problem 11.4 (1) (1 point)

Give the expanded base 6 form of 3442500_6 . Enter all digits in decimal form, that is, for A enter 10.

$$\underline{\hspace{1cm}} \cdot 6^6 + \underline{\hspace{1cm}} \cdot 6^5 + \underline{\hspace{1cm}} \cdot 6^4 + \underline{\hspace{1cm}} \cdot 6^3 + \underline{\hspace{1cm}} \cdot 6^2 + \underline{\hspace{1cm}} \cdot 6 + \underline{\hspace{1cm}} \cdot 1$$

Give 3442500_6 in decimal representation.

Problem 11.4 (2) (1 point)

Give the expanded base 12 form of $BB8848_{12}$. Enter all digits in decimal form, that is, for A enter 10.

$$\underline{\hspace{1cm}} \cdot 12^6 + \underline{\hspace{1cm}} \cdot 12^5 + \underline{\hspace{1cm}} \cdot 12^4 + \underline{\hspace{1cm}} \cdot 12^3 + \underline{\hspace{1cm}} \cdot 12^2 + \underline{\hspace{1cm}} \cdot 12 + \underline{\hspace{1cm}} \cdot 1$$

Give $BB8848_{12}$ in decimal representation.

Problem 11.4 (3) (1 point)

Give the expanded base 6 form of 105453_6 . Enter all digits in decimal form, that is, for A enter 10.

$$\underline{\hspace{1cm}} \cdot 6^6 + \underline{\hspace{1cm}} \cdot 6^5 + \underline{\hspace{1cm}} \cdot 6^4 + \underline{\hspace{1cm}} \cdot 6^3 + \underline{\hspace{1cm}} \cdot 6^2 + \underline{\hspace{1cm}} \cdot 6 + \underline{\hspace{1cm}} \cdot 1$$

Give 105453_6 in decimal representation.

Problem 11.4 (4) (1 point)

Give the expanded base 18 form of $AAGAFH7_{18}$. Enter all digits in decimal form, that is, for A enter 10.

$$\underline{\hspace{1cm}} \cdot 18^6 + \underline{\hspace{1cm}} \cdot 18^5 + \underline{\hspace{1cm}} \cdot 18^4 + \underline{\hspace{1cm}} \cdot 18^3 + \underline{\hspace{1cm}} \cdot 18^2 + \underline{\hspace{1cm}} \cdot 18 + \underline{\hspace{1cm}} \cdot 1$$

Give $AAGAFH7_{18}$ in decimal representation.

Problem 11.4 (5) (1 point)

What are the place values of a base 6 number with 5 digits?

leftmost digit $\rightarrow$ $\leftarrow$ rightmost digit

Convert these base 6 numbers to decimal numbers.

$$0_6 = ______ \quad 1_6 = ______ \quad 3_6 = ______ \quad 5_6 = ______$$

$$10_6 = ______ \quad 11_6 = ______ \quad 50_6 = ______ \quad 42_6 = ______$$

$$100_6 = ______ \quad 101_6 = ______ \quad 110_6 = ______ \quad 533_6 = ______$$

$$1000_6 = ______ \quad 1005_6 = ______ \quad 1030_6 = ______ \quad 5330_6 = ______$$

Problem 11.4 (6) (1 point)

What are the positional values of the digits of a base 16 number with 5 digits?

leftmost digit $\rightarrow$ $______ ______ ______ ______ ______ \leftarrow$ rightmost digit

Convert these base 16 numbers to decimal numbers.

$$0_{16} = ______ \quad 1_{16} = ______ \quad 7_{16} = ______ \quad F_{16} = ______$$

$$10_{16} = ______ \quad 11_{16} = ______ \quad D7_{16} = ______ \quad 37_{16} = ______$$

$$100_{16} = ______ \quad 101_{16} = ______ \quad 110_{16} = ______ \quad 813_{16} = ______$$

$$1000_{16} = ______ \quad 100F_{16} = ______ \quad 1070_{16} = ______ \quad 8130_{16} = ______$$

Problem 11.4 (7) (1 point)

Give $GA3AE62_{18}$ in decimal representation.

Problem 11.4 (8) (1 point)

Count in base 5

The characters used to represent base 5 numbers are (separate the numbers by commas):

In the first column enter the numbers in base 5 starting at 0. In the other columns enter the values for the digits of the base 5 number in decimal representation.

For your convenience the last number in each row is the corresponding decimal number.

$$\begin{array}{r} ______ 5 = \\ ______ \cdot 5^1 + \end{array}$$

$$\underline{\hspace{1cm}} \cdot 5^0 = 0$$

$$\begin{array}{l} \underline{\hspace{1cm}} \cdot 5 = \\ \underline{\hspace{1cm}} \cdot 5^1 + \\ \underline{\hspace{1cm}} \cdot 5^0 = 1 \end{array}$$

$$\begin{array}{l} \underline{\hspace{1cm}} \cdot 5 = \\ \underline{\hspace{1cm}} \cdot 5^1 + \\ \underline{\hspace{1cm}} \cdot 5^0 = 2 \end{array}$$

$$\begin{array}{l} \underline{\hspace{1cm}} \cdot 5 = \\ \underline{\hspace{1cm}} \cdot 5^1 + \\ \underline{\hspace{1cm}} \cdot 5^0 = 3 \end{array}$$

$$\begin{array}{l} \underline{\hspace{1cm}} \cdot 5 = \\ \underline{\hspace{1cm}} \cdot 5^1 + \\ \underline{\hspace{1cm}} \cdot 5^0 = 4 \end{array}$$

$$\begin{array}{l} \underline{\hspace{1cm}} \cdot 5 = \\ \underline{\hspace{1cm}} \cdot 5^1 + \\ \underline{\hspace{1cm}} \cdot 5^0 = 5 \end{array}$$

$$\begin{array}{l} \underline{\hspace{1cm}} \cdot 5 = \\ \underline{\hspace{1cm}} \cdot 5^1 + \\ \underline{\hspace{1cm}} \cdot 5^0 = 6 \end{array}$$

$$\begin{array}{l} \underline{\hspace{1cm}} \cdot 5 = \\ \underline{\hspace{1cm}} \cdot 5^1 + \\ \underline{\hspace{1cm}} \cdot 5^0 = 7 \end{array}$$

$$\begin{array}{l} \underline{\hspace{1cm}} \cdot 5 = \\ \underline{\hspace{1cm}} \cdot 5^1 + \\ \underline{\hspace{1cm}} \cdot 5^0 = 8 \end{array}$$

$$\begin{array}{l} \underline{\hspace{1cm}} \cdot 5 = \\ \underline{\hspace{1cm}} \cdot 5^1 + \\ \underline{\hspace{1cm}} \cdot 5^0 = 9 \end{array}$$

$$\begin{array}{l} \underline{\hspace{1cm}} \cdot 5 = \\ \underline{\hspace{1cm}} \cdot 5^1 + \\ \underline{\hspace{1cm}} \cdot 5^0 = 10 \end{array}$$

$$\begin{array}{l} \underline{\hspace{1cm}} \cdot 5 = \\ \underline{\hspace{1cm}} \cdot 5^1 + \\ \underline{\hspace{1cm}} \cdot 5^0 = 11 \end{array}$$

$$\underline{\hspace{1cm}} \cdot 5 =$$

$$\begin{array}{l} ___.5^1 + \\ ___.5^0 = 12 \end{array}$$

$$\begin{array}{l} ___.5 = \\ ___.5^1 + \\ ___.5^0 = 13 \end{array}$$

$$\begin{array}{l} ___.5 = \\ ___.5^1 + \\ ___.5^0 = 14 \end{array}$$

$$\begin{array}{l} ___.5 = \\ ___.5^1 + \\ ___.5^0 = 15 \end{array}$$

$$\begin{array}{l} ___.5 = \\ ___.5^1 + \\ ___.5^0 = 16 \end{array}$$

$$\begin{array}{l} ___.5 = \\ ___.5^1 + \\ ___.5^0 = 17 \end{array}$$

$$\begin{array}{l} ___.5 = \\ ___.5^1 + \\ ___.5^0 = 18 \end{array}$$

$$\begin{array}{l} ___.5 = \\ ___.5^1 + \\ ___.5^0 = 19 \end{array}$$

$$\begin{array}{l} ___.5 = \\ ___.5^1 + \\ ___.5^0 = 20 \end{array}$$

$$\begin{array}{l} ___.5 = \\ ___.5^1 + \\ ___.5^0 = 21 \end{array}$$

$$\begin{array}{l} ___.5 = \\ ___.5^1 + \\ ___.5^0 = 22 \end{array}$$

$$\begin{array}{l} ___.5 = \\ ___.5^1 + \\ ___.5^0 = 23 \end{array}$$

Solutions

Problem 11.4 (1) *Correct Answers:*

- 3
 - 4
 - 4
 - 2
 - 5
 - 0
 - 0
 - 176868
-

Problem 11.4 (2) *Correct Answers:*

- 0
 - 11
 - 11
 - 8
 - 8
 - 4
 - 8
 - 2980280
-

Problem 11.4 (3) *Correct Answers:*

- 0
 - 1
 - 0
 - 5
 - 4
 - 5
 - 3
 - 9033
-

Problem 11.4 (4) *Correct Answers:*

- 10
 - 10
 - 16
 - 10
 - 15
 - 17
 - 7
 - 360761029
-

Problem 11.4 (5) *Correct Answers:*

- 1296
- 216
- 36

- 6
- 1
- 0
- 1
- 3
- 5
- 6
- 7
- 30
- 26
- 36
- 37
- 42
- 201
- 216
- 221
- 234
- 1206

Problem 11.4 (6) *Correct Answers:*

- 65536
- 4096
- 256
- 16
- 1
- 0
- 1
- 7
- 15
- 16
- 17
- 215
- 55
- 256
- 257
- 272
- 2067
- 4096
- 4111
- 4208
- 33072

Problem 11.4 (7) *Correct Answers:*

- 563469158

Problem 11.4 (8) *Correct Answers:*

- 0, 1, 2, 3, 4

- 0
- 0
- 0
- 1
- 0
- 1
- 2
- 0
- 2
- 3
- 0
- 3
- 4
- 0
- 4
- 10
- 1
- 0
- 11
- 1
- 1
- 12
- 1
- 2
- 13
- 1
- 3
- 14
- 1
- 4
- 20
- 2
- 0
- 21
- 2
- 1
- 22
- 2
- 2
- 23
- 2
- 3
- 24
- 2
- 4
- 30
- 3

- 0
- 31
- 3
- 1
- 32
- 3
- 2
- 33
- 3
- 3
- 34
- 3
- 4
- 40
- 4
- 0
- 41
- 4
- 1
- 42
- 4
- 2
- 43
- 4
- 3

11.5 From Decimal to Base b

Problem 11.5 (1) (1 point)

With the conversion algorithm find the base 7 representation of the decimal number 66073.

Input: Base $b := \underline{\hspace{1cm}}$ and a base 10 number $a := \underline{\hspace{1cm}}$

Let $q_0 := a$.

Let $r_0 := q_0 \bmod b = \underline{\hspace{1cm}}$. Let $q_1 := a_0 \operatorname{div} b = \underline{\hspace{1cm}}$.

Let $r_1 := q_1 \bmod b = \underline{\hspace{1cm}}$. Let $q_2 := a_1 \operatorname{div} b = \underline{\hspace{1cm}}$.

Let $r_2 := q_2 \bmod b = \underline{\hspace{1cm}}$. Let $q_3 := a_2 \operatorname{div} b = \underline{\hspace{1cm}}$.

Let $r_3 := q_3 \bmod b = \underline{\hspace{1cm}}$. Let $q_4 := a_3 \operatorname{div} b = \underline{\hspace{1cm}}$.

Let $r_4 := q_4 \bmod b = \underline{\hspace{1cm}}$. Let $q_5 := a_4 \operatorname{div} b = \underline{\hspace{1cm}}$.

Let $r_5 := q_5 \bmod b = \underline{\hspace{1cm}}$. Let $q_6 := a_5 \operatorname{div} b = \underline{\hspace{1cm}}$.

Output: The expanded base 7 representation of the decimal number 66073 is:

$$\begin{aligned} 66073 &= r_5 \cdot 7^5 + r_4 \cdot 7^4 + r_3 \cdot 7^3 + r_2 \cdot 7^2 + r_1 \cdot 7^1 + r_0 \cdot 7^0 \\ &= \underline{\hspace{1cm}} \cdot 7^5 + \underline{\hspace{1cm}} \cdot 7^4 + \underline{\hspace{1cm}} \cdot 7^3 + \underline{\hspace{1cm}} \cdot 7^2 + \underline{\hspace{1cm}} \cdot 7^1 + \underline{\hspace{1cm}} \cdot 7^0 \end{aligned}$$

Now give the base 7 representation of 66073.

[Although writing leading zeros is mathematically correct, it will be marked as wrong. Do not put extra zeros in front of your answer. For example, you would write 101 instead of 0101.]

$$66073 = \underline{\hspace{1cm}}_7$$

Problem 11.5 (2) (1 point)

With the conversion algorithm find the base 13 representation of the decimal number 27322.

Input: Base $b := \underline{\hspace{1cm}}$ and a base 10 number $a := \underline{\hspace{1cm}}$

Let $q_0 := a$.

Let $r_0 := q_0 \bmod b = \underline{\hspace{1cm}}$. Let $q_1 := a_0 \operatorname{div} b = \underline{\hspace{1cm}}$.

Let $r_1 := q_1 \bmod b = \underline{\hspace{1cm}}$. Let $q_2 := a_1 \div b = \underline{\hspace{1cm}}$.

Let $r_2 := q_2 \bmod b = \underline{\hspace{1cm}}$. Let $q_3 := a_2 \div b = \underline{\hspace{1cm}}$.

Let $r_3 := q_3 \bmod b = \underline{\hspace{1cm}}$. Let $q_4 := a_3 \div b = \underline{\hspace{1cm}}$.

Output: The expanded base 13 representation of the decimal number 27322 is:

$$27322 = r_3 \cdot 13^3 + r_2 \cdot 13^2 + r_1 \cdot 13^1 + r_0 \cdot 13^0$$

$$= \underline{\hspace{1cm}} \cdot 13^3 + \underline{\hspace{1cm}} \cdot 13^2 + \underline{\hspace{1cm}} \cdot 13^1 + \underline{\hspace{1cm}} \cdot 13^0$$

Now give the base 13 representation of 27322.

[Although writing leading zeros is mathematically correct, it will be marked as wrong. Do not put extra zeros in front of your answer. For example, you would write 101 instead of 0101.

Be careful to write *A* for 10 and *B* for 11 and *C* for 12 and so on.]

$$27322 = \underline{\hspace{1cm}}_{13}$$

Problem 11.5 (3) (1 point)

With the conversion algorithm find the base 17 representation of the decimal number 50391.

Input: Base $b := \underline{\hspace{1cm}}$ and a base 10 number $a := \underline{\hspace{1cm}}$

Let $q_0 := a$.

Let $r_0 := q_0 \bmod b = \underline{\hspace{1cm}}$. Let $q_1 := a_0 \div b = \underline{\hspace{1cm}}$.

Let $r_1 := q_1 \bmod b = \underline{\hspace{1cm}}$. Let $q_2 := a_1 \div b = \underline{\hspace{1cm}}$.

Let $r_2 := q_2 \bmod b = \underline{\hspace{1cm}}$. Let $q_3 := a_2 \div b = \underline{\hspace{1cm}}$.

Let $r_3 := q_3 \bmod b = \underline{\hspace{1cm}}$. Let $q_4 := a_3 \div b = \underline{\hspace{1cm}}$.

Output: The expanded base 17 representation of the decimal number 50391 is:

$$50391 = r_3 \cdot 17^3 + r_2 \cdot 17^2 + r_1 \cdot 17^1 + r_0 \cdot 17^0$$

$$= \underline{\hspace{1cm}} \cdot 17^3 + \underline{\hspace{1cm}} \cdot 17^2 + \underline{\hspace{1cm}} \cdot 17^1 + \underline{\hspace{1cm}} \cdot 17^0$$

Now give the base 17 representation of 50391.

[Although writing leading zeros is mathematically correct, it will be marked as wrong. Do not put extra

zeros in front of your answer. For example, you would write 101 instead of 0101.
Be careful to write *A* for 10 and *B* for 11 and *C* for 12 and so on.]

$$50391 = \text{_____}_{17}$$

Problem 11.5 (4) (1 point)

Convert these base numbers from decimal to base 6 representation.

[Although writing leading zeros is mathematically correct, it will be marked as wrong. Do not put extra zeros in front of your answer. So write 101 instead of 0101 etc.]

$$1 = \text{_____}_6 \quad 2 = \text{_____}_6$$

$$6 = \text{_____}_6 \quad 6 = \text{_____}_6$$

$$36 = \text{_____}_6 \quad 36 = \text{_____}_6$$

Problem 11.5 (5) (1 point)

Convert these base numbers from decimal to base 13 representation.

[Although writing leading zeros is mathematically correct, it will be marked as wrong. Do not put extra zeros in front of your answer. So write 101 instead of 0101 etc.]

$$1 = \text{_____}_{13} \quad 10 = \text{_____}_{13}$$

$$13 = \text{_____}_{13} \quad 13 = \text{_____}_{13}$$

$$169 = \text{_____}_{13} \quad 2028 = \text{_____}_{13}$$

Problem 11.5 (6) (1 point)

Convert these numbers from base 10 to base 17 representation.

[Although writing leading zeros is mathematically correct, it will be marked as wrong. Do not put extra zeros in front of your answer. So write 101_{17} instead of 0101_{17} etc.]

$$1 = \text{_____}_{17} \quad 1 = \text{_____}_{17}$$

$$17 = \text{_____}_{17} \quad 119 = \text{_____}_{17}$$

$$289 = \text{_____}_{17} \quad 3757 = \text{_____}_{17}$$

Problem 11.5 (7) (1 point)

Convert from decimal to base 5 representation.

[Although writing leading zeros is mathematically correct, it will be marked as wrong. Do not put extra zeros in front of your answer. So write 101 instead of 0101 etc.]

$$1472 = \text{_____}_5$$

Problem 11.5 (8) (1 point)

Convert from decimal to base 15 representation.

[Although writing leading zeros is mathematically correct, it will be marked as wrong. Do not put extra zeros in front of your answer. So write 101 instead of 0101 etc.]

$$9984788 = \text{_____}_{15}$$

Solutions

Problem 11.5 (1) *Correct Answers:*

- 7
- 66073
- 0
- 9439
- 3
- 1348
- 4
- 192
- 3
- 27
- 6
- 3
- 3
- 0
- 3
- 6
- 3
- 4
- 3
- 0
- 363430

Problem 11.5 (2) *Correct Answers:*

- 13
- 27322
- 9
- 2101
- 8
- 161
- 5
- 12
- 12
- 0
- 12
- 5
- 8
- 9
- C589

Problem 11.5 (3) *Correct Answers:*

- 17
- 50391
- 3
- 2964
- 6
- 174
- 4
- 10
- 10
- 0
- 10
- 4
- 6
- 3
- A463

Problem 11.5 (4) *Correct Answers:*

- 1
- 2
- 10
- 10
- 100
- 100

Problem 11.5 (5) *Correct Answers:*

- 1
- A
- 10
- 10
- 100
- C00

Problem 11.5 (6) *Correct Answers:*

- 1
- 1
- 10
- 70
- 100
- D00

Problem 11.5 (7) *Correct Answers:*

- 21342

Problem 11.5 (8) *Correct Answers:*

- D236C8

Chapter 12

Applications of other Bases

1. Images
2. Colors
3. Text

12.1 Images

Problem 12.1 (1) (1 point)

Represent each row of the image by a decimal number.

Black is represented by 1. The pixel on the left is represented by the most significant binary digit.

	decimal			
0 0 0 0	—			
0 1 1 0	—			
1 0 1 1	—			
1 1 1 1	—			

Problem 12.1 (2) (1 point)

Represent each row of the image by a decimal number.

Black is represented by 1. The pixel on the left is represented by the most significant binary digit.

2^5	2^4	2^3	2^2	2^1	2^0	decimal
1	0	0	1	0	1	—
0	0	1	0	1	1	—
0	1	1	1	0	0	—

Problem 12.1 (3) (1 point)

Represent each row of the image by a decimal number.

Black is represented by 1. The pixel on the left is represented by the most significant binary digit.

2^3	2^2	2^1	2^0	decimal
				—
				—
				—
				—

Problem 12.1 (4) (1 point)

Represent each row of the image by a binary and a decimal number.

Black is represented by 1. The pixel on the left is represented by the most significant binary digit.

2^4	2^3	2^2	2^1	2^0	binary	decimal
					—	—
					—	—
					—	—
					—	—

Problem 12.1 (5) (1 point)

Represent each row of the image by a decimal number.

Black is represented by 1. The pixel on the left is represented by the most significant binary digit.

2^4	2^3	2^2	2^1	2^0	decimal
					—
					—
					—

Problem 12.1 (6) (1 point)

An image showing a letter is encoded into numbers.

In the encoding a 0 corresponds to a white and a 1 to a black pixel. When converting to decimal the most significant binary digit was on the left.

2

5

7

5

5

What is the letter ? ____

Problem 12.1 (7) (1 point)

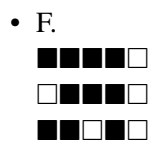
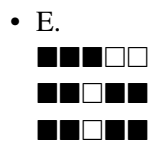
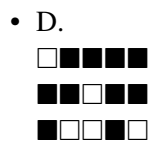
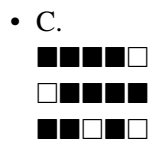
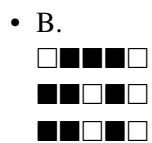
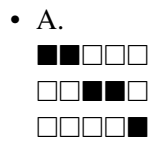
An image has been encoded into numbers.

In the encoding 0 corresponded to white and 1 to black pixels. When converting to decimal the most significant binary digit was on the left.

24

6
1

Which of these images corresponds to the numbers above ?



Problem 12.1 (8) (1 point)

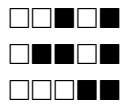
An image has been encoded into numbers.

In the encoding 0 corresponded to white and 1 to black pixels. When converting to decimal the most significant binary digit was on the left.

5
13
3

Which of these images corresponds to the numbers above ?

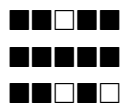
- A.



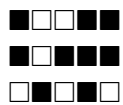
- B.



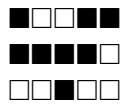
- C.



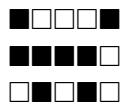
- D.



- E.



- F.



Problem 12.1 (9) (1 point)

An image showing a letter is encoded into numbers.

In the encoding a 0 corresponds to a white and a 1 to a black pixel. When converting to decimal the most significant binary digit was on the left.

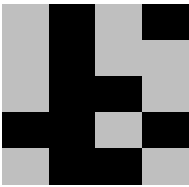
3
4
4
4
3

What is the letter ? ____

Problem 12.1 (10) (1 point)

Represent each row of the image by a binary and a decimal number.

Black is represented by 1. The pixel on the left is represented by the most significant binary digit.

	binary	decimal
	_____	_____
	_____	_____
	_____	_____
	_____	_____
	_____	_____

Solutions

Problem 12.1 (1) Correct Answers:

Hint: The weights of the columns are the powers of 2. For example

2^4	2^3	2^2	2^1	2^0	
1	0	0	1	0	$10010_2 = 1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 = 18$
0	1	0	1	1	$01011_2 = 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 11$

Correct Answers:

- 0
- 6
- 11
- 15

Problem 12.1 (2) Correct Answers:

Hint: The weights of the columns are the powers of 2. For example

2^4	2^3	2^2	2^1	2^0	
1	0	0	1	0	$10010_2 = 1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 = 18$
0	1	0	1	1	$01011_2 = 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 11$

Correct Answers:

- 37
- 11
- 28

Problem 12.1 (3) Correct Answers:

Hint: The weights of the columns are the powers of 2. For example

2^4	2^3	2^2	2^1	2^0	
					$10010_2 = 1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 = 18$
					$01011_2 = 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 11$

Correct Answers:

- 7
- 0
- 11
- 4

Problem 12.1 (4) Correct Answers:

Hint: The weights of the columns are the powers of 2. For example

2^4	2^3	2^2	2^1	2^0	
					$10010_2 = 1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 = 18$
					$01011_2 = 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 11$

Correct Answers:

- 1000
- 8
- 1000
- 8
- 0
- 0
- 10
- 2

Problem 12.1 (5) Correct Answers:

Hint: The weights of the columns are the powers of 2. For example

2^4	2^3	2^2	2^1	2^0	
					$10010_2 = 1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 = 18$
					$01011_2 = 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 11$

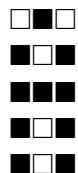
Correct Answers:

- 17
- 3
- 17

Problem 12.1 (6) Correct Answers:

Solution:

The image is:



Thus the letter is 'A'.

Correct Answers:

- A

Problem 12.1 (7) Correct Answers:

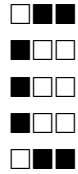
- A

Problem 12.1 (8) Correct Answers:

- A

Problem 12.1 (9) *Correct Answers:***Solution:**

The image is:



Thus the letter is 'C'.

Correct Answers:

- C

Problem 12.1 (10) *Correct Answers:*

Hint: The weights of the columns are the powers of 2. For example

2^4	2^3	2^2	2^1	2^0	
■	■	■	■	■	$10010_2 = 1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 = 18$
■	■	■	■	■	$01011_2 = 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 11$

Correct Answers:

- 101
- 5
- 100
- 4
- 110
- 6
- 1101
- 13
- 110
- 6

12.2 Colors

Problem 12.2 (1) (1 point)

Select the RGB hex triplets that correspond to the given colors.

1. ____  black
2. ____  yellow
3. ____  red
4. ____  green

Problem 12.2 (2) (1 point)

Select the colors that best describe the colors represented by the RGB hex triplets.

1. ____ #FF0000
2. ____ #FFFF00
3. ____ #A0A0A0
4. ____ #111111

Problem 12.2 (3) (1 point)

In each line determine whether the color on the left is darker than, lighter than, or the same as the color on the right.

#C0C0C0 ____ #0C0C0C.

[select: | **is darker than** | **is lighter than** | **is the same as**]

#818181 ____ #8B8B8B.

[select: | **is darker than** | **is lighter than** | **is the same as**]

#7E7E7E ____ #000000.

[select: | **is darker than** | **is lighter than** | **is the same as**]

#686868 ____ #000000.

[select: | **is darker than** | **is lighter than** | **is the same as**]

#3D3D3D ____ #D3D3D3.

[select: | **is darker than** | **is lighter than** | **is the same as**]

Problem 12.2 (4) (1 point)

In each line determine whether the color on the left is darker than, lighter than, or the same as the color on the right.

#696969 ____ #6F6F6F.

[select: | **is darker than** | **is lighter than** | **is the same as**]

#3D3D3D ____ #D3D3D3.

[select: | **is darker than** | **is lighter than** | **is the same as**]

#777777 ____ #EEEEEE.

[select: | **is darker than** | **is lighter than** | **is the same as**]

#C2C2C2 ____ #2C2C2C.

[select: | **is darker than** | **is lighter than** | **is the same as**]

#0A0A0A ____ #DCDCDC.

[select: | **is darker than** | **is lighter than** | **is the same as**]

Problem 12.2 (5) (1 point)

Select the colors that best describe the colors represented by the RGB hex triplets.

1. ____ #FF0000
2. ____ #A0A0A0
3. ____ #FF00FF
4. ____ #828282

Problem 12.2 (6) (1 point)

Select the RGB hex triplets that correspond to the given colors.

1. ____ white
2. ____  green
3. ____  blue
4. ____  red

Problem 12.2 (7) (1 point)

Select the RGB hex triplets that correspond to the given colors.

1. ____  blue
2. ____  black
3. ____ white
4. ____  magenta

Problem 12.2 (8) (1 point)

Select the colors that best describe the colors represented by the RGB hex triplets.

1. ____ #FFFF00
2. ____ #FFFFFF
3. ____ #FF0000
4. ____ #111111

Problem 12.2 (9) (1 point)

In each line determine whether the color on the left is darker than, lighter than, or the same as the color on the right.

#D0D0D0 ____ #0D0D0D.

[select: | **is darker than** | **is lighter than** | **is the same as**]

#B1B1B1 ____ #1B1B1B.

[select: | **is darker than** | **is lighter than** | **is the same as**]

#282828 ____ #FFFFFF.

[select: | **is darker than** | **is lighter than** | **is the same as**]

#6C6C6C ____ #6B6B6B.

[select: | **is darker than** | **is lighter than** | **is the same as**]

#010101 ____ #FFFFFF.

[select: | **is darker than** | **is lighter than** | **is the same as**]

Problem 12.2 (10) (1 point)

In each line determine whether the color on the left is darker than, lighter than, or the same as the color on the right.

#FFFFFF ____ #A6A6A6.

[select: | **is darker than** | **is lighter than** | **is the same as**]

#959595 ____ #2A2A2A.

[select: | **is darker than** | **is lighter than** | **is the same as**]

#696969 ____ #4B4B4B.

[select: | **is darker than** | **is lighter than** | **is the same as**]

#AAAAAA ____ #888888.

[select: | **is darker than** | **is lighter than** | **is the same as**]

#868686 ____ #D5D5D5.

[select: | **is darker than** | **is lighter than** | **is the same as**]

Problem 12.2 (11) (1 point)

Select the colors that best describe the colors represented by the RGB hex triplets.

1. ____ #FFFFFF
2. ____ #0000FF
3. ____ #FFFF00
4. ____ #FF00FF

Problem 12.2 (12) (1 point)

Select the RGB hex triplets that correspond to the given colors.

1. ____  yellow
2. ____  magenta
3. ____  black
4. ____  cyan

Solutions

Problem 12.2 (1) *Correct Answers:*

- 000000
 - FFFF00
 - FF0000
 - 00FF00
-

Problem 12.2 (2) *Correct Answers:*

- red
 - yellow
 - grey
 - grey
-

Problem 12.2 (3) *Correct Answers:*

Hint: All colors in this problems are shades of grey.

Correct Answers:

- is lighter than
 - is darker than
 - is lighter than
 - is lighter than
 - is darker than
-

Problem 12.2 (4) *Correct Answers:*

Hint: All colors in this problems are shades of grey.

Correct Answers:

- is darker than
 - is darker than
 - is darker than
 - is lighter than
 - is darker than
-

Problem 12.2 (5) *Correct Answers:*

- red
- grey
- magenta
- grey

Problem 12.2 (6) *Correct Answers:*

- FFFFFFFF
- 00FF00
- 0000FF
- FF0000

Problem 12.2 (7) *Correct Answers:*

- 0000FF
- 000000
- FFFFFFFF
- FF00FF

Problem 12.2 (8) *Correct Answers:*

- yellow
- white
- red
- grey

Problem 12.2 (9) *Correct Answers:*

Hint: All colors in this problems are shades of grey.

Correct Answers:

- is lighter than
- is lighter than
- is darker than
- is lighter than
- is darker than

Problem 12.2 (10) *Correct Answers:*

Hint: All colors in this problems are shades of grey.

Correct Answers:

- is lighter than
- is lighter than
- is lighter than
- is lighter than
- is darker than

Problem 12.2 (11) *Correct Answers:*

- white
- blue
- yellow
- magenta

Problem 12.2 (12) *Correct Answers:*

- FFFF00
- FF00FF
- 000000
- 00FFFF

Encoding the word hares we obtain _____

Problem 12.3 (4) (1 point)

A word was encoded as an integer by

(1) applying the encoding function C to the characters,

$C : \{-, a, b, \dots, z\} \rightarrow \{0, 1, 2, 3, \dots, 26\}$ with $C(-) = 0, C(a) = 1, \dots, C(z) = 26$.

(2) considering the resulting integers as the digits of a number in base 27 representation such that the last letter of the word corresponds to the unit digit, and

(3) then taking the decimal representation.

The word encoded in 7219805 is _____.

Problem 12.3 (5) (1 point)

Words can be encoded in the integer by applying the encoding function C :

$C : \{-, a, b, \dots, z\} \rightarrow \{0, 1, 2, 3, \dots, 26\}$ with $C(-) = 0, C(a) = 1, \dots, C(z) = 26$.

And then considering the resulting integers as the digits of a base 27 number such that the last letter of the word corresponds to the unit digit, and then taking the decimal representation.

Encoding the word worms we obtain _____

Problem 12.3 (6) (1 point)

A word was encoded as an integer by

(1) applying the encoding function C to the characters,

$C : \{-, a, b, \dots, z\} \rightarrow \{0, 1, 2, 3, \dots, 26\}$ with $C(-) = 0, C(a) = 1, \dots, C(z) = 26$.

(2) considering the resulting integers as the digits of a number in base 27 representation such that the last letter of the word corresponds to the unit digit, and

(3) then taking the decimal representation.

The word encoded in 10256069 is _____.

Solutions

Problem 12.3 (1) *Correct Answers:*

- 8
 - 15
 - 18
 - 19
 - 5
 - horse
-

Problem 12.3 (2) *Correct Answers:*

- 19
 - 20
 - 1
 - 18
 - 388602
-

Problem 12.3 (3) *Correct Answers:*

Hint: We encode hares as

$$C(\mathbf{h}) \cdot 27^4 + C(\mathbf{a}) \cdot 27^3 + C(\mathbf{r}) \cdot 27^2 + C(\mathbf{e}) \cdot 27 + C(\mathbf{s}).$$

Correct Answers:

- 4284487
-

Problem 12.3 (4) *Correct Answers:*

- mouse
-

Problem 12.3 (5) *Correct Answers:*

Hint: We encode worms as

$$C(\mathbf{w}) \cdot 27^4 + C(\mathbf{o}) \cdot 27^3 + C(\mathbf{r}) \cdot 27^2 + C(\mathbf{m}) \cdot 27 + C(\mathbf{s}).$$

Correct Answers:

- 12531880
-

Problem 12.3 (6) *Correct Answers:*

- shark

Chapter 13

Binary Operations

1. Definition of Binary Operation
2. Associativity
3. Identity
4. Inverses
5. Commutativity

13.1 Definition of Binary Operation

Problem 13.1 (1) (1 point)

Let the binary operation $\star$ (star) on the set $H = \{b, c, d, e, f, g\}$ be defined by:

$\star$	b	c	d	e	f	g
b	b	b	b	b	b	b
c	c	e	b	c	e	b
d	d	c	g	e	f	b
e	e	c	b	e	c	b
f	f	e	g	c	d	b
g	g	b	g	b	g	b

We read $f \star g$ as f star g.

Find the following.

$$f \star g = \underline{\hspace{1cm}}$$

$$g \star f = \underline{\hspace{1cm}}$$

$$e \star d = \underline{\hspace{1cm}}$$

$$d \star e = \underline{\hspace{1cm}}$$

$$(e \star d) \star e = \underline{\hspace{1cm}}$$

$$e \star (d \star e) = \underline{\hspace{1cm}}$$

Problem 13.1 (2) (1 point)

Fill in the operation table for the binary operation $\oplus$ on the set $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1)\}$ defined by

$$(a,b) \oplus (c,d) = ((a+c) \bmod 2, (b+d) \bmod 2).$$

$\oplus$	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	—	(0,1)	(1,0)	(1,1)
(0,1)	—	(0,0)	(1,1)	—
(1,0)	(1,0)	—	—	—
(1,1)	—	—	(0,1)	—

Problem 13.1 (3) (1 point)

Fill in the operation table for the binary operation $\oplus$ on the set $\mathbb{Z}_4$ defined by $a \oplus b = (a+b) \bmod 4$:

The left column represents the a values and the top row represents the b values.

$\oplus$	0	1	2	3
0	0	—	2	3
1	1	—	3	0
2	2	—	0	1
3	—	—	—	—

Problem 13.1 (4) (1 point)

Let the binary operation $\star$ (star) on the set $A = \{b, c, d, e, f, g, h, i, j, k\}$ be defined by:

$\star$	b	c	d	e	f	g	h	i	j	k
b	b	c	d	e	f	g	h	i	j	k
c	c	e	g	i	k	b	d	f	h	j
d	d	g	j	b	e	h	k	c	f	i
e	e	i	b	f	j	c	g	k	d	h
f	f	k	e	j	d	i	c	h	b	g
g	g	b	h	c	i	d	j	e	k	f
h	h	d	k	g	c	j	f	b	i	e
i	i	f	c	k	h	e	b	j	g	d
j	j	h	f	d	b	k	i	g	e	c
k	k	j	i	h	g	f	e	d	c	b

We read $g \star j$ as g star j .

Find the following.

$$g \star j = \underline{\hspace{1cm}}$$

$$j \star g = \underline{\hspace{1cm}}$$

$$e \star h = \underline{\hspace{1cm}}$$

$$h \star k = \underline{\hspace{1cm}}$$

$$(e \star h) \star k = \underline{\hspace{1cm}}$$

$$e \star (h \star k) = \underline{\hspace{1cm}}$$

Problem 13.1 (5) (1 point)

Fill in the operation table for the binary operation $\otimes$ on the set $\mathbb{Z}_3$ defined by $a \otimes b = (a \cdot b) \bmod 3$:

The left column represents the a values and the top row represents the b values.

$\otimes$	0	1	2
0	0	0	—
1	—	—	—
2	0	2	—

Solutions

Problem 13.1 (1) *Correct Answers:*

- b
 - g
 - b
 - e
 - b
 - e
-

Problem 13.1 (2) *Correct Answers:*

- (0,0)
 - (0,1)
 - (1,0)
 - (1,1)
 - (0,0)
 - (0,1)
 - (1,1)
 - (1,0)
 - (0,0)
-

Problem 13.1 (3) *Correct Answers:*

- 1
 - 2
 - 3
 - 3
 - 0
 - 1
 - 2
-

Problem 13.1 (4) *Correct Answers:*

- k
- k
- g
- e
- f
- f

Problem 13.1 (5) *Correct Answers:*

- 0
- 0
- 1
- 2
- 1

13.2 Associativity

Problem 13.2 (1) (1 point)

Let S be a set and let $*$: $S \times S \rightarrow S$ be a binary operation on S . We read $a * b$ as 'a star b'.

If $\underline{(A)} = (a * b) * c \underline{(B)}$, then the binary operation $*$ is called $\underline{(C)}$.

(A): [select: | $a * (b * c)$ | $(a * b) * c$ | $(a * b) * (a * c)$ | $(a * b) * c$]

(B): [select: | for all a in S and some b in S | for some a in S , all b in S , and all c in S | for all a in S , all b in S , and all c in S | for $a=1$ and $b=2$ and $c=3$]

(C): [select: | associative | commutative | distributive | transitive]

Problem 13.2 (2) (1 point)

Determine which of these operations are associative.

1. ___ The operation $\ominus : \mathbb{Z}_{14} \times \mathbb{Z}_{14} \rightarrow \mathbb{Z}_{14}$ given by $a \ominus b = (a - b) \bmod 14$.
2. ___ The operation $\star : \mathbb{Z}_{16}^{\otimes} \times \mathbb{Z}_{16}^{\otimes} \rightarrow \mathbb{Z}_{16}^{\otimes}$ given by $a \star b = (a^b) \bmod 16$.
3. ___ The operation subtraction $- : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$.

Problem 13.2 (3) (1 point)

Let a be an integer.

Suppose that the remainder when a is divided by 5 is 2 and the remainder when b is divided by 5 is 3.

That is, $a \bmod 5 = 2$ and $b \bmod 5 = 3$.

Find:

$$(a + a) \bmod 5 = \underline{\hspace{2cm}}$$

$$(a + b) \bmod 5 = \underline{\hspace{2cm}}$$

$$(a \cdot b) \bmod 5 = \underline{\hspace{2cm}}$$

$$(a + 4) \bmod 5 = \underline{\hspace{2cm}}$$

$$(4 \cdot b) \bmod 5 = \underline{\hspace{2cm}}$$

Solutions

Problem 13.2 (1) *Correct Answers:*

- $a * (b * c)$
- for all a in S , all b in S , and all c in S
- associative

Problem 13.2 (2) *Correct Answers:*

Hint: If the operation is not associative, this can be easily shown by finding a counterexample.

Correct Answers:

- N
- N
- N

Problem 13.2 (3) *Correct Answers:*

- 4
- 0
- 1
- 1
- 2

13.3 Identity

Problem 13.3 (1) (1 point)

Let S be a set and let $*$: $S \times S \rightarrow S$ be a binary operation on S . We read $a * b$ as 'a star b'.

An element e in S is an identity element with respect to $*$ if (A) for (B).

(A): [select: | $(a * b) * c = a * (b * c)$ | $a * b = b * a$ | $a * e = a$ and $e * a = a$ | $a * b = e$ and $b * a = e$]

(B): [select: | all a in S | one a in S | all a in S and all b in S | one a in S and one b in S | all a in S , all b in S , and all c in S | one a in S , one b in S , and one c in S | the identity e with respect to $*$ in S | all e in S]

Problem 13.3 (2) (1 point)

Fill in the operation table for the binary operation $\oplus$ on the set $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1)\}$ defined by $(a,b) \oplus (c,d) = ((a+c) \bmod 2, (b+d) \bmod 2)$:

$\oplus$	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	—	(0,1)	(1,0)	—
(0,1)	(0,1)	—	(1,1)	—
(1,0)	(1,0)	—	—	—
(1,1)	(1,1)	—	(0,1)	—

Complete the following:

In $\mathbb{Z}_2 \times \mathbb{Z}_2$ with respect to $\oplus$ _____. [select: | the identity element is (0,0) | the identity element is (1,1) | the identity element is (1,0) | the identity element is (0,1) | there is no identity element]

Problem 13.3 (3) (1 point)

Fill in the operation table for the binary operation $\ominus$ on the set $\mathbb{Z}_5^\times$ defined by $a \ominus b = (a - b) \bmod 5$:

$\ominus$	1	2	3	4
1	—	—	—	—
2	—	—	—	—
3	—	—	—	—
4	—	—	—	—

Complete the following:

In $\mathbb{Z}_5^\times$ with respect to $\ominus$ _____. [select: | **the identity element is 1** | **there is no identity element**]

Problem 13.3 (4) (1 point)

Decide whether the following statements are true or false. If the statement is false give a counterexample, otherwise leave the field empty.

(1) Let the binary operation $\ominus : \mathbb{Z}_4 \times \mathbb{Z}_4 \rightarrow \mathbb{Z}_4$ be given by $a \ominus b = (a - b) \bmod 4$.

[select: | **The statement is true.** | **The statement is false.**]

The identity element with respect to $\ominus$ is 1.

Counterexample: The statement is false, because for $b := ___ \in \mathbb{Z}_4$ we have $1 \ominus b \neq b$.

(2) Let the binary operation $\oplus : \mathbb{Z}_8 \times \mathbb{Z}_8 \rightarrow \mathbb{Z}_8$ be given by $a \oplus b = (a + b) \bmod 8$.

[select: | **The statement is true.** | **The statement is false.**]

The identity element with respect to $\oplus$ is 6.

Counterexample: The statement is false, because for $b := ___ \in \mathbb{Z}_8$ we have $6 \oplus b \neq b$.

(3) Let the binary operation $\otimes : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ be given by $a \otimes b = (a \cdot b)$.

[select: | **The statement is true.** | **The statement is false.**]

The identity element with respect to $\otimes$ is -5 .

Counterexample: The statement is false, because for $b := ___ \in \mathbb{Z}$ we have $-5 \otimes b \neq b$.

Problem 13.3 (5) (1 point)

Let S be a set and let $*$: $S \times S \rightarrow S$ be a binary operation on S . We read $a * b$ as 'a star b'.

An element e in S is an identity element with respect to $*$ if $\underline{\hspace{1cm}}^{(A)}$ for $\underline{\hspace{1cm}}^{(B)}$.

(A): [select: | $(a * b) * c = a * (b * c)$ | $a * b = b * a$ | $a * e = a$ and $e * a = a$ | $a * b = e$ and $b * a = e$]

(B): [select: | **all a in S** | **one a in S** | **all a in S and all b in S** | **one a in S and one b in S** | **all a in S,**

all b in S , and all c in S | one a in S , one b in S , and one c in S | the identity e with respect to $*$ in S | all e in S]

Determine for which of these operations there is an identity in the corresponding set.

1. ___ The operation $\ominus : \mathbb{Z}_3 \times \mathbb{Z}_3 \rightarrow \mathbb{Z}_3$ given by $a \ominus b = (a - b) \bmod 3$.
2. ___ The operation $\star : \mathbb{Z}_3^\otimes \times \mathbb{Z}_3^\otimes \rightarrow \mathbb{Z}_3^\otimes$ given by $a \star b = (a^b) \bmod 3$.
3. ___ The operation $\oplus : \mathbb{Z}_3 \times \mathbb{Z}_3 \rightarrow \mathbb{Z}_3$ given by $a \oplus b = (a + b) \bmod 3$.

Problem 13.3 (6) (1 point)

Decide whether the following statements are true or false. If the statement is false give a counterexample, otherwise leave the field empty.

(1) Let the binary operation $\otimes : \mathbb{Z}_{11} \times \mathbb{Z}_{11} \rightarrow \mathbb{Z}_{11}$ be given by $a \otimes b = (a \cdot b) \bmod 11$.

[select: | **The statement is true.** | **The statement is false.**]

The identity element with respect to $\otimes$ is 8.

Counterexample: The statement is false, because for $b := __ \in \mathbb{Z}_{11}$ we have $8 \otimes b \neq b$.

(2) Let the binary operation $\ominus : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ be given by $a \ominus b = (a - b)$.

[select: | **The statement is true.** | **The statement is false.**]

The identity element with respect to $\ominus$ is -1 .

Counterexample: The statement is false, because for $b := __ \in \mathbb{Z}$ we have $-1 \ominus b \neq b$.

(3) Let the binary operation $\star : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ be given by $a \star b = (a^b)$.

[select: | **The statement is true.** | **The statement is false.**]

The identity element with respect to $\star$ is 5.

Counterexample: The statement is false, because for $b := __ \in \mathbb{Z}$ we have $5 \star b \neq b$.

Problem 13.3 (7) (1 point)

What is the identity in the following sets with respect to the given operation.

1. ___ $\mathbb{Z}_3$ with the operation $*$ defined by $a*b = (a \cdot b) \bmod 3$
2. ___ $\mathbb{Z}_6$ with the operation $*$ defined by $a*b = (a - b) \bmod 6$
3. ___ $\mathbb{Z}_6$ with the operation $*$ defined by $a*b = (a + b) \bmod 6$
4. ___ $\mathbb{Z}$ with the operation $*$ defined by $a*b = a \cdot b$
5. ___ $\mathbb{Z}$ with subtraction

Solutions

Problem 13.3 (1) *Correct Answers:*

- $a * e = a$ and $e * a = a$
 - all a in S
-

Problem 13.3 (2) *Correct Answers:*

- $(0,0)$
 - $(1,1)$
 - $(0,0)$
 - $(1,0)$
 - $(1,1)$
 - $(0,0)$
 - $(0,1)$
 - $(1,0)$
 - $(0,0)$
 - the identity element is $(0,0)$
-

Problem 13.3 (3) *Correct Answers:*

- 0
 - 4
 - 3
 - 2
 - 1
 - 0
 - 4
 - 3
 - 2
 - 1
 - 0
 - 4
 - 3
 - 2
 - 1
 - 0
 - there is no identity element
-

Problem 13.3 (4)

- (1) **Hint:** An element $e \in \mathbb{Z}_4$ is the identity with respect to $\ominus$ if $e \ominus b = b$ and $b \ominus e = b$ for all $b \in \mathbb{Z}_4$.

Correct Answers:

The statement is false.

Any $b \in \mathbb{Z}_3$ yields a counterexample.

For example, $b = 3$ is a counterexample, because

$$1 \ominus b = 1 \ominus 3 = (1 - 3) \bmod 4 = -2 \bmod 4 = 2 \neq 3 = b$$

- (2) **Hint:** An element $e \in \mathbb{Z}_8$ is the identity with respect to $\oplus$ if $e \oplus b = b$ and $b \oplus e = b$ for all $b \in \mathbb{Z}_8$.

Correct Answers:

The statement is false.

Any $b \in \mathbb{Z}_8$ yields a counterexample.

For example, $b = 2$ is a counterexample, because

$$6 \oplus b = 6 \oplus 2 = (6 + 2) \bmod 8 = 8 \bmod 8 = 0 \neq 2 = b$$

- (3) **Hint:** An element $e \in \mathbb{Z}$ is the identity with respect to $\otimes$ if $e \otimes b = b$ and $b \otimes e = b$ for all $b \in \mathbb{Z}$.

Correct Answers:

The statement is false.

Any $b \in \mathbb{Z}$ with $b \neq 0$ yields a counterexample.

For example, $b = 1$ is a counterexample, because then

$$(-5) \otimes b = (-5) \otimes 1 = (-5) \cdot 1 = -5 \neq 1 = b$$

Problem 13.3 (5) *Correct Answers:*

- $a * e = a$ and $e * a = a$
 - all a in S
 - N
 - N
 - 0
-

Problem 13.3 (6)

- (1) **Hint:** An element $e \in \mathbb{Z}_{11}$ is the identity with respect to $\otimes$ if $e \otimes b = b$ and $b \otimes e = b$ for all $b \in \mathbb{Z}_{11}$.

Correct Answers:

The statement is false.

All $b \in \mathbb{Z}_{11}$ with $b \neq 0$ yield a counterexample.

For example $b = 3$ is a counterexample, because

$$8 \otimes b = 8 \otimes 3 = (8 \cdot 3) \bmod 11 = 24 \bmod 11 = 2 \neq 3 = b$$

- (2) **Hint:** An element $e \in \mathbb{Z}$ is the identity with respect to $\ominus$ if $e \ominus b = b$ and $b \ominus e = b$ for all $b \in \mathbb{Z}$.

Correct Answers:

The statement is false.

All $b \in \mathbb{Z}$ yield a counterexample.

For example $b = 3$ is a counterexample, because

$$(-1) \ominus b = (-1) \ominus 3 = -1 - 3 = -4 \neq 2 = b$$

- (3) **Hint:** An element $e \in \mathbb{Z}$ is the identity with respect to $\star$ if $e \star b = b$ and $b \star e = b$ for all $b \in \mathbb{Z}$.

Correct Answers:

The statement is false.

All $b \in \mathbb{Z}$ yield a counterexample.

For example $b = 2$ is a counterexample, because then

$$5 \star b = 5 \star 2 = 5^2 = 25 \neq 2 = b$$

Problem 13.3 (7) *Correct Answers:*

Hint: Binary operations based on addition (+) and multiplication ($\cdot$) 'inherit' properties from these operations on the integers. One of the 'inherited' properties is the identity element.

In the cases where there is no identity element, it only takes a few tries to find a counterexample.

- 1
- N
- 0
- 1
- N

13.4 Inverses

Problem 13.4 (1) (1 point)

Definition

Let S be a set and let $*$: $S \times S \rightarrow S$ be a binary operation on S . We read $a * b$ as **a star b**.

Let e be ____.

[select: | **the identity with respect to $*$ in S** | **some element in S** | **some odd element in S** | **some even element in S** | **some green element in S**]

An element b in S is an inverse of a in S with respect to $*$ if ____.

[select: | $(a * b) * c = a * (b * c)$ | $a * b = b * a$ | $a * e = a$ and $e * a = a$ | $a * b = e$ and $b * a = e$]

Problem 13.4 (2) (1 point)

Decide whether the following statements are true or false.

(i) There exists an integer a such that $a + 2 = 0$.

[select: | **The statement is true.** | **The statement is false.**]

If the statement is true, give an integer for which it is true: $a =$ ____

(ii) There exists an integer a such that $a \cdot (-1) = 1$.

[select: | **The statement is true.** | **The statement is false.**]

If the statement is true, give an integer for which it is true: $a =$ ____

(iii) There exists an integer a such that $a + 11 = 11$.

[select: | **The statement is true.** | **The statement is false.**]

If the statement is true, give an integer for which it is true: $a =$ ____

Problem 13.4 (3) (1 point)

Fill in the operation table for the binary operation $\oplus$ on the set

$$\mathbb{Z}_3 \times \mathbb{Z}_2 = \{(0, 0), (0, 1), (1, 0), (1, 1), (2, 0), (2, 1), \}$$

defined by $(a,b) \oplus (c,d) = ((a+c) \bmod 3, (b+d) \bmod 2)$:

$\oplus$	(0,0)	(0,1)	(1,0)	(1,1)	(2,0)	(2,1)
(0,0)	—	—	(1,0)	—	—	(2,1)
(0,1)	(0,1)	—	(1,1)	(1,0)	—	(2,0)
(1,0)	(1,0)	(1,1)	(2,0)	(2,1)	—	(0,1)
(1,1)	—	(1,0)	(2,1)	(2,0)	(0,1)	(0,0)
(2,0)	(2,0)	—	—	(0,1)	(1,0)	(1,1)
(2,1)	(2,1)	(2,0)	(0,1)	(0,0)	—	—

Complete the following:

In $\mathbb{Z}_3 \times \mathbb{Z}_2$ with respect to $\oplus$ _____. [select: | **the identity element is (0,0)** | **the identity element is (1,1)** | **the identity element is (1,0)** | **the identity element is (0,1)** | **there is no identity element**]

Find the inverses of the elements of $\mathbb{Z}_3 \times \mathbb{Z}_2$ with respect to $\oplus$.

The inverse of (0,0) is _____.

The inverse of (0,1) is _____.

The inverse of (1,0) is _____.

The inverse of (1,1) is _____.

The inverse of (2,0) is _____.

The inverse of (2,1) is _____.

Problem 13.4 (4) (1 point)

Fill in the operation table for the binary operation $\oplus$ on the set

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1), \}$$

defined by $(a,b) \oplus (c,d) = ((a+c) \bmod 2, (b+d) \bmod 2)$:

$\oplus$	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,1)	—	—
(0,1)	(0,1)	—	—	(1,0)
(1,0)	(1,0)	—	—	(0,1)
(1,1)	—	(1,0)	(0,1)	—

Complete the following:

In $\mathbb{Z}_2 \times \mathbb{Z}_2$ with respect to $\oplus$ _____. [select: | **the identity element is (0,0)** | **the identity element is (1,1)** | **the identity element is (1,0)** | **the identity element is (0,1)** | **there is no identity element**]

Find the inverses of the elements of $\mathbb{Z}_2 \times \mathbb{Z}_2$ with respect to $\oplus$.

The inverse of (0,0) is _____.

The inverse of (0,1) is _____.

The inverse of (1,0) is _____.

The inverse of (1,1) is _____.

Problem 13.4 (5) (1 point)

Fill in the operation table for the binary operation $\oplus$ on the set $\mathbb{Z}_3$ defined by $a \oplus b = (a + b) \bmod 3$:

$\oplus$	0	1	2
0	_____	_____	_____
1	_____	2	_____
2	2	0	_____

Complete the following:

In $\mathbb{Z}_3$ with respect to $\oplus$ _____.

[select: | **the identity element is 0** | **the identity element is 1** | **there is no identity element**]

Find the inverses of the elements of $\mathbb{Z}_3$ with respect to $\oplus$. If an element does not have an inverse answer 'none'.

The inverse of 0 is _____.

The inverse of 1 is _____.

The inverse of 2 is _____.

Problem 13.4 (6) (1 point)

For each operation find the identity and decide whether the statement is true or false.

(1) Let the binary operation $\oplus : \mathbb{Z}_4 \times \mathbb{Z}_4 \rightarrow \mathbb{Z}_4$ be given by $a \oplus b = (a + b) \bmod 4$. The identity with respect to $\oplus$ is ____.

[select: | **The statement is true.** | **The statement is false.**] The inverse of 0 with respect to $\oplus$ is 0.

(2) Let the binary operation $\otimes : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ be given by $a \otimes b = (a \cdot b)$. The identity with respect to $\otimes$ is ____.

[select: | **The statement is true.** | **The statement is false.**] The inverse of 1 with respect to $\otimes$ is 5.

(3) Let the binary operation $\oplus : \mathbb{Z}_4 \times \mathbb{Z}_4 \rightarrow \mathbb{Z}_4$ be given by $a \oplus b = (a + b) \bmod 4$. The identity with respect to $\oplus$ is ____.

[select: | **The statement is true.** | **The statement is false.**] The inverse of 1 with respect to $\oplus$ is 0.

Problem 13.4 (7) (1 point)

Fill in the operation table for the binary operation $\oplus$ on the set $\mathbb{Z}_7$ defined by $a \oplus b = (a + b) \bmod 7$:

$\oplus$	0	1	2	3	4	5	6
0	—	—	2	3	4	5	—
1	—	2	3	—	5	6	—
2	2	—	—	5	—	0	—
3	—	—	5	6	0	1	2
4	4	5	6	0	1	—	3
5	—	—	0	—	2	—	4
6	—	—	—	—	—	4	—

Complete the following:

In $\mathbb{Z}_7$ with respect to $\oplus$ ____.

[select: | **the identity element is 0** | **the identity element is 1** | **there is no identity element**]

Find the inverses of the elements of $\mathbb{Z}_7$ with respect to $\oplus$. If an element does not have an inverse answer 'none'.

The inverse of 0 is ____.

The inverse of 1 is ____.

The inverse of 2 is ____.

The inverse of 3 is ____.

The inverse of 4 is ____.

The inverse of 5 is ____.

The inverse of 6 is ____.

Solutions

Problem 13.4 (1) *Correct Answers:*

- the identity with respect to $*$ in S
 - $a * b = e$ and $b * a = e$
-

Problem 13.4 (2) *Correct Answers:*

- The statement is true
 - -2
 - The statement is true
 - -1
 - The statement is true
 - 0
-

Problem 13.4 (3) *Correct Answers:*

- $(0,0)$
 - $(0,1)$
 - $(1,1)$
 - $(2,0)$
 - $(0,0)$
 - $(2,1)$
 - $(0,0)$
 - $(1,1)$
 - $(2,1)$
 - $(0,0)$
 - $(1,1)$
 - $(1,0)$
 - the identity element is $(0,0)$
 - $(0,0)$
 - $(0,1)$
 - $(2,0)$
 - $(2,1)$
 - $(1,0)$
 - $(1,1)$
-

Problem 13.4 (4) *Correct Answers:*

- $(1,0)$
- $(1,1)$
- $(0,0)$
- $(1,1)$
- $(1,1)$
- $(0,0)$
- $(1,1)$
- $(0,0)$
- the identity element is $(0,0)$
- $(0,0)$

- $(0, 1)$
- $(1, 0)$
- $(1, 1)$

Problem 13.4 (5) *Correct Answers:*

- 0
- 1
- 2
- 1
- 0
- 1
- the identity element is 0
- 0
- 2
- 1

Problem 13.4 (6) *Correct Answers:*

For (1):

Hint: An element $b \in \mathbb{Z}_4$ is the inverse of $a \in \mathbb{Z}_4$ with respect to $\oplus$ if $a \oplus b = 0$ and $b \oplus a = 0$.

For (2):

Hint: An element $b \in \mathbb{N}$ is the inverse of $a \in \mathbb{N}$ with respect to $\otimes$ if $a \otimes b = 1$ and $b \otimes a = 1$.

For (3):

Hint: An element $b \in \mathbb{Z}_4$ is the inverse of $a \in \mathbb{Z}_4$ with respect to $\oplus$ if $a \oplus b = 0$ and $b \oplus a = 0$.

Correct Answers:

- 0
- The statement is true.
- 1
- The statement is false.
- 0
- The statement is false.

Problem 13.4 (7) *Correct Answers:*

- 0
- 1
- 6
- 1
- 4
- 0
- 3
- 4
- 6
- 1
- 3

- 4
- 2
- 5
- 6
- 1
- 3
- 6
- 0
- 1
- 2
- 3
- 5
- the identity element is 0
- 0
- 6
- 5
- 4
- 3
- 2
- 1

13.5 Commutativity

Problem 13.5 (1) (1 point)

Let S be a set and let $*$: $S \times S \rightarrow S$ be a binary operation on S . We read $a * b$ as 'a star b'.

The operation $*$ is commutative if (A) for (B).

(A): [select: | $(a * b) * c = a * (b * c)$ | $a * b = b * a$ | $a * e = a$ and $e * a = a$ | $a * b = e$ and $b * a = e$]

(B): [select: | **all a in S** | **one a in S** | **all a in S and all b in S** | **one a in S and one b in S** | **all a in S, all b in S, and all c in S** | **one a in S, one b in S, and one c in S** | **the identity e with respect to * in S** | **all e in S**]

Problem 13.5 (2) (1 point)

Fill in the operation table for the binary operation $\otimes$ on the set $\mathbb{Z}_4$ defined by $a \otimes b = (a \cdot b) \bmod 4$:

$\otimes$	0	1	2	3
0	—	—	0	0
1	—	1	—	—
2	0	—	—	2
3	0	—	—	—

Complete the following:

The operation $\otimes$ is _____. [select: | **commutative** | **not commutative**]

Problem 13.5 (3) (1 point)

Determine which of these operations are commutative.

Hint: if you are not sure, try a few examples, to try to find a counterexample

1. ____ The operation $\oplus : \mathbb{Z}_7 \times \mathbb{Z}_7 \rightarrow \mathbb{Z}_7$ given by $a \oplus b = (a + b) \bmod 7$.
2. ____ The operation $\ominus : \mathbb{Z}_{14} \times \mathbb{Z}_{14} \rightarrow \mathbb{Z}_{14}$ given by $a \ominus b = (a - b) \bmod 14$.
3. ____ The operation $\otimes : \mathbb{Z}_5^\otimes \times \mathbb{Z}_5^\otimes \rightarrow \mathbb{Z}_5^\otimes$ given by $a \otimes b = (a \cdot b) \bmod 5$.

Problem 13.5 (4) (1 point)

Complete the following table to make $*$ into a commutative operation on the set $\{a, b, c, d\}$:

$*$	b	a	d	c
b	a	b	—	d
a	—	c	—	—
d	d	d	a	b
c	—	a	—	c

Problem 13.5 (5) (1 point)

Let $\square$ on the set $E = \{p, a, q, b, r\}$ be defined by:

$\square$	p	a	q	b	r
p	p	p	p	p	p
a	p	a	q	b	r
q	p	q	r	a	b
b	p	b	a	r	q
r	p	r	b	q	a

The operation $\square$ on the set E is _____. [select: | **commutative** | **not commutative**]

Problem 13.5 (6) (1 point)

Decide whether the following binary operations are commutative. If the binary operation is not commutative, give a counterexample, otherwise leave the field empty.

(1) Let the binary operation $\star : \mathbb{Z}_5 \times \mathbb{Z}_5 \rightarrow \mathbb{Z}_5$ be given by $a \star b = (a^b) \bmod 5$.

The binary operation $\star$ is _____. [select: | **commutative** | **not commutative**]

Counterexample: The statement is false, because for $a = ___ \in \mathbb{Z}_5$ we have $a \star 3 \neq 3 \star a$.

(2) Let the binary operation $\oplus : \mathbb{Z}_{15} \times \mathbb{Z}_{15} \rightarrow \mathbb{Z}_{15}$ be given by $a \oplus b = (a + b) \bmod 15$.

The binary operation $\oplus$ is _____. [select: | **commutative** | **not commutative**]

Counterexample: The statement is false, because for $a = ___ \in \mathbb{Z}_{15}$ we have $a \oplus 5 \neq 5 \oplus a$.

(3) Let the binary operation $\otimes : \mathbb{Z}_{11} \times \mathbb{Z}_{11} \rightarrow \mathbb{Z}_{11}$ be given by $a \otimes b = (a \cdot b) \bmod 11$.

The binary operation $\otimes$ is _____. [select: | **commutative** | **not commutative**]

Counterexample: The statement is false, because for $a = ___ \in \mathbb{Z}_{11}$ we have $a \otimes 3 \neq 3 \otimes a$.

Solutions

Problem 13.5 (1) *Correct Answers:*

- $a * b = b * a$
 - all a in S and all b in S
-

Problem 13.5 (2) *Correct Answers:*

- 0
 - 0
 - 0
 - 2
 - 3
 - 2
 - 0
 - 3
 - 2
 - 1
 - commutative
-

Problem 13.5 (3) *Correct Answers:*

- C
 - N
 - C
-

Problem 13.5 (4) *Correct Answers:*

- d
 - b
 - d
 - a
 - d
 - b
-

Problem 13.5 (5) *Correct Answers:*

- commutative

Problem 13.5 (6) Correct Answers:**For (1):****Hint:** The binary operation $\star$ is commutative if $a \star b = b \star a$ for all $a \in \mathbb{Z}_5$ and for all $b \in \mathbb{Z}_5$.**For (2):****Hint:** The binary operation $\oplus$ is commutative if $a \oplus b = b \oplus a$ for all $a \in \mathbb{Z}_{15}$ and for all $b \in \mathbb{Z}_{15}$.**For (3):****Hint:** The binary operation $\otimes$ is commutative if $a \otimes b = b \otimes a$ for all $a \in \mathbb{Z}_{11}$ and for all $b \in \mathbb{Z}_{11}$.*Correct Answers:*

- not commutative
- $a = 2$ is a counterexample because

$$a \star 3 = 2 \star 3 = 2^3 \bmod 5 = 8 \bmod 5 = 3$$

and

$$3 \star a = 3 \star 2 = 2^3 \bmod 5 = 9 \bmod 5 = 4$$

and thus

$$3 = a \star 3 \neq 3 \star a = 4$$

- commutative
- N/A
- commutative
- N/A

Chapter 14

Groups

1. Definition of Group
2. Examples of Groups
3. Modular Arithmetic
4. Additive Groups
5. Multiplicative Groups

14.1 Definition of Group

Problem 14.1 (1) (1 point)

Let S be a set and let $*$: $S \times S \rightarrow S$ be a binary operation on S . We read $a * b$ as 'a star b'.

The operation $*$ is associative if (A) for (B).

(A): [select: | $(a * b) * c = a * (b * c)$ | $a * b = b * a$ | $a * e = a$ and $e * a = a$ | $a * b = e$ and $b * a = e$]

(B): [select: | **all a in S** | **one a in S** | **all a in S and all b in S** | **one a in S and one b in S** | **all a in S, all b in S, and all c in S** | **one a in S, one b in S, and one c in S** | **the identity e with respect to * in S** | **all e in S**]

The operation $*$ is commutative if (A) for (B).

(A): [select: | $(a * b) * c = a * (b * c)$ | $a * b = b * a$ | $a * e = a$ and $e * a = a$ | $a * b = e$ and $b * a = e$]

(B): [select: | **all a in S** | **one a in S** | **all a in S and all b in S** | **one a in S and one b in S** | **all a in S, all b in S, and all c in S** | **one a in S, one b in S, and one c in S** | **the identity e with respect to * in S** | **all e in S**]

An element e in S is an identity with respect to $*$ if (A) for (B).

(A): [select: | $(a * b) * c = a * (b * c)$ | $a * b = b * a$ | $a * e = a$ and $e * a = a$ | $a * b = e$ and $b * a = e$]

(B): [select: | **all a in S** | **one a in S** | **all a in S and all b in S** | **one a in S and one b in S** | **all a in S, all b in S, and all c in S** | **one a in S, one b in S, and one c in S** | **the identity e with respect to * in S** | **all e in S**]

If an identity with respect to $*$ exists then it is unique. So we can talk about the identity with respect to $*$.

An element b in S is an inverse of a in S if where e is the identity with respect to $*$.

[select: | $(a * b) * c = a * (b * c)$ | $a * b = b * a$ | $a * e = a$ and $e * a = a$ | $a * b = e$ and $b * a = e$]

Problem 14.1 (2) (1 point)

A set S with a binary operation $*$ on S is a commutative group if (A) with respect to $*$ in S and (B) with respect to $*$ in S and (C).

(A): [select: | **a complement** | **an element** | **an identity** | **an inverse** | **a set** | **an operation**]

(B): [select: | **a complement** | **an element** | **an identity** | **an inverse** | **a set** | **an operation**]

(C): [select: | **associative and commutative** | **associative and transitive** | **commutative and symmetric**]

Problem 14.1 (3) (1 point)

Let G be a set and $\star : G \times G \rightarrow G$ a binary operation.

Match the statements below by entering the letter of the corresponding name of the property on the right.

- ___ 1. For all $a \in G$, $b \in G$, and $c \in G$ we have $a \star (b \star c) = (a \star b) \star c$.
- ___ 2. Let e be the identity with respect to $\star$. For all $a \in G$ there exists a $b \in G$ such that $a \star b = e$ and $b \star a = e$.
- ___ 3. There exists $e \in G$ such that for all $a \in G$ we have $a \star e = a$ and $e \star a = e$.
- ___ 4. For all $a \in G$ and $b \in G$ we have $a \star b = b \star a$.

- A. Commutative property of $\star$
- B. Existence of inverses with respect to $\star$
- C. Associative property of $\star$
- D. Existence of an identity with respect to $\star$

Solutions

Problem 14.1 (1) *Correct Answers:*

- $(a * b) * c = a * (b * c)$
 - all a in S , all b in S , all c in S
 - $a * b = b * a$
 - all a in S and all b in S
 - $a * e = a$ and $e * a = a$
 - all a in S
 - $a * b = e$ and $b * a = e$
-

Problem 14.1 (2) *Correct Answers:*

- an identity
 - an inverse
 - associative and commutative
-

Problem 14.1 (3) *Correct Answers:*

- C
- B
- D
- A

14.2 Examples of Groups

Problem 14.2 (1) (1 point)

Complete the operation table for the binary operation $\otimes$ on the set $\mathbb{Z}_8$ defined by $a \otimes b = (a \cdot b) \bmod 8$:

$\otimes$	0	1	2	3	4	5	6	7
0	0	0	—	—	0	—	0	—
1	0	1	2	—	—	—	6	7
2	0	2	4	6	0	—	—	6
3	0	—	6	—	—	7	2	5
4	—	4	—	—	—	—	—	4
5	0	5	—	7	4	1	—	3
6	0	6	—	—	—	6	—	2
7	0	—	6	—	4	—	2	—

Complete the following:

(1) In $\mathbb{Z}_8$ with respect to $\otimes$ ____.

[select: | **the identity element is 0** | **the identity element is 1** | **there is no identity element**]

(2) Find the inverses of the elements of $\mathbb{Z}_8$ with respect to $\otimes$. If an element does not have an inverse answer: **none**.

The inverse of 0 is ____.

The inverse of 1 is ____.

The inverse of 2 is ____.

The inverse of 3 is ____.

The inverse of 4 is ____.

The inverse of 5 is ____.

The inverse of 6 is ____.

The inverse of 7 is ____.

With respect to $\otimes$ ____.

[select: | **each element has an inverse** | **at least one element does not have an inverse** | **there is no**

identity, so inverses are not defined]

(3) $\otimes$ is associative

(4) $\otimes$ is ____.

[select: | **commutative** | **not commutative**]

Now decide whether $(\mathbb{Z}_8, \otimes)$ is a commutative group:

The set $\mathbb{Z}_8$ with the operation $\otimes$ is ____.

[select: | **a commutative group** | **not a commutative group**]

Problem 14.2 (2) (1 point)

Fill in the operation table for the binary operation $\otimes$ on the set $\mathbb{Z}_3^\otimes$ defined by $a \otimes b = (a \cdot b) \bmod 3$:

$\otimes$	1	2
1	1	___
2	2	1

Complete the following:

(1) in $\mathbb{Z}_3^\otimes$ with respect to $\otimes$ ____.

[select: | **the identity element is 1** | **there is no identity element**]

(2) Find the inverses of the elements of $\mathbb{Z}_3^\otimes$ with respect to $\otimes$. If an element does not have an inverse answer: **none**.

The inverse of 1 is ____.

The inverse of 2 is ____.

With respect to $\otimes$ ____.

[select: | **each element has an inverse** | **at least one element does not have an inverse** | **there is no identity, so inverses are not defined**]

(3) $\otimes$ is associative.

(4) $\otimes$ is ____.

[select: | **commutative** | **not commutative**]

Decide whether $(\mathbb{Z}_3^\otimes, \otimes)$ is a commutative group:

The set $\mathbb{Z}_3^\otimes$ with the operation $\otimes$ is ____.

[select: | **a commutative group** | **not a commutative group**]

Problem 14.2 (3) (1 point)

Complete the operation table for the binary operation $\ominus$ on the set $\mathbb{Z}_2$ defined by $a \ominus b = (a - b) \bmod 2$:

$\ominus$	0	1
0	0	—
1	—	0

Complete the following:

(1) In $\mathbb{Z}_2$ with respect to $\ominus$ ____.

[select: | **the identity element is 0** | **the identity element is 1** | **there is no identity element**]

(2) Find the inverses of the elements of $\mathbb{Z}_2$ with respect to $\ominus$. If an element does not have an inverse answer: **none**.

The inverse of 0 is ____.

The inverse of 1 is ____.

With respect to $\ominus$ ____.

[select: | **each element has an inverse** | **at least one element does not have an inverse** | **there is no identity, so inverses are not defined**]

(3) $\ominus$ is associative.

(4) $\ominus$ is ____.

[select: | **commutative** | **not commutative**]

Now decide whether $(\mathbb{Z}_2, \ominus)$ is a commutative group:

The set $\mathbb{Z}_2$ with the operation $\ominus$ is ____.

[select: | **a commutative group** | **not a commutative group**]

Problem 14.2 (4) (1 point)

Fill in the operation table for the binary operation $\star$ on the set $S = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2), \}$ defined by $(a,b) \star (c,d) = ((a+c) \bmod 2, (b+d) \bmod 3)$:

$\star$	(0,0)	(0,1)	(0,2)	(1,0)	(1,1)	(1,2)
(0,0)	(0,0)	(0,1)	—	(1,0)	(1,1)	(1,2)
(0,1)	(0,1)	—	—	(1,1)	—	(1,0)
(0,2)	—	(0,0)	(0,1)	—	(1,0)	—
(1,0)	—	—	—	—	—	—
(1,1)	(1,1)	—	—	—	(0,2)	—
(1,2)	(1,2)	(1,0)	—	(0,2)	—	(0,1)

Complete the following:

(1) In $\mathbb{Z}_2 \times \mathbb{Z}_3$ with respect to the operation $\star$ ____.

[select: | **the identity element is (0,0)** | **the identity element is (1,1)** | **the identity element is (1,0)** | **the identity element is (0,1)** | **there is no identity element**]

(2) In $\mathbb{Z}_2 \times \mathbb{Z}_3$ ____.

[select: | **each element has an inverse** | **at least one element does not have an inverse** | **there is no identity, so inverses are not defined**]

with respect to the operation $\star$.

(3) The operation $\star$ is associative.

(4) The operation $\star$ is ____.

[select: | **commutative** | **not commutative**]

Conclude whether $(\mathbb{Z}_2 \times \mathbb{Z}_3, \star)$ is a commutative group:

The set $\mathbb{Z}_2 \times \mathbb{Z}_3$ with the operation $\star$ is ____.

[select: | **a commutative group** | **not a commutative group**]

Problem 14.2 (5) (1 point)

Let $D = \{ p, q, r, s \}$. Let the binary operation $\square$ on D be defined by

$\square$	p	q	r	s
p	p	q	r	s
q	q	r	s	p
r	r	s	p	q
s	s	p	q	r

Complete the following:

(1) In the set D with respect to the operation $\square$ ____.

[select: | **the identity element is p** | **the identity element is q** | **the identity element is r** | **the identity element is s** | **there is no identity element**]

(2) Find the inverses of the elements of D with respect to $\square$. If an element does not have an inverse answer: **none**.

The inverse of p is ____.

The inverse of q is ____.

The inverse of r is ____.

The inverse of s is ____.

In the set D ____.

[select: | **each element has an inverse** | **at least one element does not have an inverse** | **there is no identity, so inverses are not defined**]

with respect to the operation $\square$.

(3) The operation $\square$ is associative.

(4) The operation $\square$ is ____.

[select: | **commutative** | **not commutative**]

Conclude whether $(D, \square)$ is a commutative group:

The set D with the operation $\square$ is ____.

[select: | **a commutative group** | **not a commutative group**]

Problem 14.2 (6) (1 point)

Complete the operation table for the binary operation $\otimes$ on the set $\mathbb{Z}_7$ defined by $a \otimes b = (a \cdot b) \bmod 7$:

$\otimes$	0	1	2	3	4	5	6
0	—	—	0	0	0	0	—
1	—	1	—	—	—	—	6
2	0	2	—	—	1	—	5
3	—	3	—	2	—	—	4
4	0	—	—	—	2	6	3
5	0	5	3	1	—	—	—
6	0	6	—	4	—	—	—

Complete the following:

(1) In $\mathbb{Z}_7$ with respect to $\otimes$ ____.

[select: | **the identity element is 0** | **the identity element is 1** | **there is no identity element**]

(2) Find the inverses of the elements of $\mathbb{Z}_7$ with respect to $\otimes$. If an element does not have an inverse answer: **none**.

The inverse of 0 is ____.

The inverse of 1 is ____.

The inverse of 2 is ____.

The inverse of 3 is ____.

The inverse of 4 is ____.

The inverse of 5 is ____.

The inverse of 6 is ____.

With respect to $\otimes$ ____.

[select: | **each element has an inverse** | **at least one element does not have an inverse** | **there is no identity, so inverses are not defined**]

(3) $\otimes$ is associative

(4) $\otimes$ is ____.

[select: | **commutative** | **not commutative**]

Now decide whether $(\mathbb{Z}_7, \otimes)$ is a commutative group:

The set $\mathbb{Z}_7$ with the operation $\otimes$ is ____.

[select: | **a commutative group** | **not a commutative group**]

Solutions

Problem 14.2 (1) *Correct Answers:*

- 0
- 0
- 0
- 0
- 3
- 4
- 5
- 2
- 4
- 3
- 1
- 4
- 0
- 0
- 4
- 0
- 4
- 0
- 2
- 6
- 4
- 2
- 0
- 4
- 7
- 5
- 3
- 1
- the identity element is 1
- none
- 1
- none
- 3
- none
- 5
- none
- 7
- at least one element does not have an inverse
- commutative
- not a commutative group

Problem 14.2 (2) *Correct Answers:*

- 2
- the identity element is 1

- 1
- 2
- each element has an inverse
- commutative
- a commutative group

Problem 14.2 (3) *Correct Answers:*

- 1
- 1
- the identity element is 0
- 0
- 1
- each element has an inverse
- commutative
- a commutative group

Problem 14.2 (4) *Correct Answers:*

- (0,2)
- (0,2)
- (0,0)
- (1,2)
- (0,2)
- (1,2)
- (1,1)
- (1,0)
- (1,1)
- (1,2)
- (0,0)
- (0,1)
- (0,2)
- (1,2)
- (1,0)
- (0,1)
- (0,0)
- (1,1)
- (0,0)
- the identity element is (0,0)
- each element has an inverse
- commutative
- a commutative group

Problem 14.2 (5) *Correct Answers:*

- the identity element is p
- p
- s
- r

- q
- each element has an inverse
- commutative
- a commutative group

Problem 14.2 (6) *Correct Answers:*

- 0
- 0
- 0
- 0
- 2
- 3
- 4
- 5
- 4
- 6
- 3
- 0
- 6
- 5
- 1
- 4
- 1
- 5
- 6
- 4
- 2
- 5
- 3
- 2
- 1
- the identity element is 1
- none
- 1
- 4
- 5
- 2
- 3
- 6
- at least one element does not have an inverse
- commutative
- not a commutative group

14.3 Modular Arithmetic

Problem 14.3 (1) (1 point)

Let $a := 7021$, $b := 656$, $c := 26$, and $d := 7918$.

Compute:

$$a \bmod 7 = \underline{\hspace{2cm}}$$

$$b \bmod 7 = \underline{\hspace{2cm}}$$

$$c \bmod 7 = \underline{\hspace{2cm}}$$

$$d \bmod 7 = \underline{\hspace{2cm}}$$

Now use these to compute the following:

$$(a + b) \bmod 7 = \underline{\hspace{2cm}}$$

$$(c + d) \bmod 7 = \underline{\hspace{2cm}}$$

$$(b \cdot c) \bmod 7 = \underline{\hspace{2cm}}$$

$$(d \cdot a) \bmod 7 = \underline{\hspace{2cm}}$$

Problem 14.3 (2) (1 point)

Perform the following computations:

$$2103 \bmod 11 = \underline{\hspace{2cm}}$$

$$5313 \bmod 11 = \underline{\hspace{2cm}}$$

$$8983 \bmod 11 = \underline{\hspace{2cm}}$$

Now use these results to find the following:

$$(2103 \cdot 5313) \bmod 11 = \underline{\hspace{2cm}}$$

$$(5313 + 8983) \bmod 11 = \underline{\hspace{2cm}}$$

$$((2103 \cdot 5313) + 8983) \bmod 11 = \underline{\hspace{2cm}}$$

$$(2103 + 5313 + 8983) \bmod 11 = \underline{\hspace{2cm}}$$

Problem 14.3 (3) (1 point)

Let a be an integer.

Suppose that the remainder when a is divided by 8 is 3 and the remainder when b is divided by 8 is 4.

That is, $a \bmod 8 = 3$ and $b \bmod 8 = 4$.

Find:

$$(a + a) \bmod 8 = \underline{\hspace{2cm}}$$

$$(a + b) \bmod 8 = \underline{\hspace{1cm}}$$

$$(a \cdot b) \bmod 8 = \underline{\hspace{1cm}}$$

$$(a + 3) \bmod 8 = \underline{\hspace{1cm}}$$

$$(3 \cdot b) \bmod 8 = \underline{\hspace{1cm}}$$

Problem 14.3 (4) (1 point)

The remainder when a is divided by 42 is 5 and the remainder when b is divided by 42 is 11.

That is, $a \bmod 42 = 5$ and $b \bmod 42 = 11$.

Find:

$$(a + a) \bmod 42 = \underline{\hspace{1cm}}$$

$$(a + b) \bmod 42 = \underline{\hspace{1cm}}$$

$$(a \cdot b) \bmod 42 = \underline{\hspace{1cm}}$$

$$(a + 10) \bmod 42 = \underline{\hspace{1cm}}$$

$$(10 \cdot b) \bmod 42 = \underline{\hspace{1cm}}$$

Problem 14.3 (5) (1 point)

Let $\oplus : \mathbb{Z}_{47} \times \mathbb{Z}_{47} \rightarrow \mathbb{Z}_{47}$ be defined by $a \oplus b = (a + b) \bmod 47$.

Compute

$$9 \oplus 45 = \underline{\hspace{1cm}}$$

$$45 \oplus 9 = \underline{\hspace{1cm}}$$

$$(22 \oplus 21) \oplus 17 = \underline{\hspace{1cm}}$$

$$22 \oplus (21 \oplus 17) = \underline{\hspace{1cm}}$$

Problem 14.3 (6) (1 point)

Let $\otimes : \mathbb{Z}_{11}^{\otimes} \times \mathbb{Z}_{11}^{\otimes} \rightarrow \mathbb{Z}_{11}^{\otimes}$ be defined by $a \otimes b = (a \cdot b) \bmod 11$.

Compute

$$8 \otimes 9 = \underline{\hspace{1cm}}$$

$$4 \otimes 3 = \underline{\hspace{1cm}}$$

$$10 \otimes 6 = \underline{\hspace{1cm}}$$

$$7 \otimes 9 = \underline{\hspace{1cm}}$$

$$(3 \otimes 1) \otimes 8 = \underline{\hspace{1cm}}$$

$$3 \otimes (1 \otimes 8) = \underline{\hspace{1cm}}$$

Problem 14.3 (7) (1 point)

What is the identity in the following sets with respect to the given operation.

1. $\underline{\hspace{1cm}} \mathbb{Z}_4$ with the operation $*$ defined by $a*b = (a \cdot b) \bmod 4$
2. $\underline{\hspace{1cm}} \mathbb{Z}$ with the operation $*$ defined by $a*b = a \cdot b$
3. $\underline{\hspace{1cm}} \mathbb{Z}$ with addition
4. $\underline{\hspace{1cm}} \mathbb{Z}_4$ with the operation $*$ defined by $a*b = (a + b) \bmod 4$
5. $\underline{\hspace{1cm}} \mathbb{Z}_2^{\otimes}$ with the operation $*$ defined by $a*b = (a \cdot b) \bmod 2$

Problem 14.3 (8) (1 point)

Consider the binary operation $+: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$.

The identity with respect to $+$ in $\mathbb{Z}$ is $\underline{\hspace{1cm}}$.

The inverse of 39 with respect to $+$ in $\mathbb{Z}$ is $\underline{\hspace{1cm}}$.

Solutions

Problem 14.3 (1) *Correct Answers:*

- 0
 - 5
 - 5
 - 1
 - 5
 - 6
 - 4
 - 0
-

Problem 14.3 (2) *Correct Answers:*

- 2
 - 0
 - 7
 - 0
 - 7
 - 7
 - 9
-

Problem 14.3 (3) *Correct Answers:*

- 6
 - 7
 - 4
 - 6
 - 4
-

Problem 14.3 (4) *Correct Answers:*

- 10
- 16
- 13
- 15
- 26

Problem 14.3 (5) *Correct Answers:*

- 7
- 7
- 13
- 13

Problem 14.3 (6) *Correct Answers:*

- 6
- 1
- 5
- 8
- 2
- 2

Problem 14.3 (7) *Correct Answers:*

Hint: Binary operations based on addition (+) and multiplication ($\cdot$) 'inherit' properties from these operations on the integers. One of the 'inherited' properties is the identity element.

In the cases where there is no identity element, it only takes a few tries to find a counterexample.

Correct Answers:

- 1
- 1
- 0
- 0
- 1

Problem 14.3 (8) *Correct Answers:*

Hint: An element $e \in \mathbb{Z}$ is the identity with respect to $+$ if $a + e = a$ and $e + a = a$ for all $a \in \mathbb{Z}$.

An element $b \in \mathbb{Z}$ is the inverse of $a \in \mathbb{Z}$ with respect to $+$ if $a + b = e$ and $b + a = e$.

Make sure that your answer is an element of $\mathbb{Z}$.

Correct Answers:

- 0
- -39

14.4 Additive Groups

Problem 14.4 (1) (1 point)

Complete the operation table for the binary operation $\oplus$ on the set $\mathbb{Z}_4$ defined by $a \oplus b = (a + b) \bmod 4$:

$\oplus$	0	1	2	3
0	___	1	2	3
1	1	2	3	___
2	___	3	___	1
3	___	___	___	___

Complete the following:

(1) In $\mathbb{Z}_4$ with respect to $\oplus$ ____.

[select: | **the identity element is 0** | **the identity element is 1** | **there is no identity element**]

(2) Find the inverses of the elements of $\mathbb{Z}_4$ with respect to $\oplus$. If an element does not have an inverse answer 'none'.

The inverse of 0 is ____.

The inverse of 1 is ____.

The inverse of 2 is ____.

The inverse of 3 is ____.

With respect to $\oplus$ ____.

[select: | **each element has an inverse** | **at least one element does not have an inverse** | **there is no identity, so inverses are not defined**]

(3) $\oplus$ is associative.

(4) $\oplus$ is ____.

[select: | **commutative** | **not commutative**]

Now decide whether $(\mathbb{Z}_4, \oplus)$ is a commutative group:

The set $\mathbb{Z}_4$ with the operation $\oplus$ is ____.

[select: | **a commutative group** | **not a commutative group**]

Problem 14.4 (2) (1 point)

Find the inverses of the elements of $\mathbb{Z}_{22}$ with respect to

$\oplus : \mathbb{Z}_{22} \times \mathbb{Z}_{22} \rightarrow \mathbb{Z}_{22}$ defined by $a \oplus b = a + b \bmod 22$.

The inverse of 14 is ____.

The inverse of 11 is ____.

The inverse of 7 is ____.

The inverse of 6 is ____.

Problem 14.4 (3) (1 point)

Let m be a natural number. Let $S = \{0, 1, 2, 3, \dots, m-1\}$. Let $\oplus : S \times S \rightarrow S$ be given by $a \oplus b = (a+b) \bmod m$.

We show that $(S, \oplus)$ is a group.

(a) Because $a \oplus 0 = \underline{(A)}$ and $0 \oplus a = \underline{(B)}$ for all a in S , the element $\underline{(C)}$ is the $\underline{(D)}$ with respect to the operation $\oplus$.

(A): [select: | **a** | **a-1** | **0** | **1** | **2** | **m-a** | **a-m**]

(B): [select: | **a** | **a-1** | **0** | **1** | **2** | **m-a** | **a-m**]

(C): [select: | **a** | **a-1** | **0** | **1** | **2** | **m-a** | **a-m**]

(D): [select: | **analogue** | **identity** | **inverse** | **opposite**]

(b) For all a in S we have $a \oplus \underline{(A)} = 0$ and $\underline{(B)} \oplus a = 0$.
Thus each a in S has an $\underline{(C)}$ with respect to the operation $\oplus$.

(A): [select: | **a** | **a-1** | **0** | **1** | **2** | **m-a** | **a-m**]

(B): [select: | **a** | **a-1** | **0** | **1** | **2** | **m-a** | **a-m**]

(C): [select: | **analogue** | **identity** | **inverse** | **opposite**]

(c) The addition of integers is associative. That means $\underline{\quad^{(A)}\quad}$ for all integers a, b, and c.
 Thus for all a, b, and c in S we have $(a \oplus b) \oplus c = \underline{\quad^{(B)}\quad} = \underline{\quad^{(C)}\quad} = a \oplus (b \oplus c)$.

(A): [select: | **$(a+b)+c = a+(b+c)$** | **$a+b = b+a$** | **$a+0 = a$ and $0+a = a$** | **$a+b = 0$ and $b+a = 0$**]

(B): [select: | **$((a+b)+c) \bmod m$** | **$(a+(b+c)) \bmod m$** | **$(a+b) \bmod m$** | **$(b+a) \bmod m$** | **$(a(b+c)) \bmod m$** | **$(ab+ac) \bmod m$**]

(C): [select: | **$((a+b)+c) \bmod m$** | **$(a+(b+c)) \bmod m$** | **$(a+b) \bmod m$** | **$(b+a) \bmod m$** | **$(a(b+c)) \bmod m$** | **$(ab+ac) \bmod m$**]

Hence the operation $\oplus$ is ____.

[select: | **associative** | **commutative** | **disruptive** | **distributive** | **orderly**]

(d) The addition of integers is commutative. That means $\underline{\quad(A)\quad}$ for all integers a and b.
 Thus for all a and b in S we have $a \oplus b = \underline{\quad(B)\quad} = \underline{\quad(C)\quad} = b \oplus a$.

(A): [select: | $(a+b)+c = a+(b+c)$ | $a+b = b+a$ | $a+0 = a$ and $0+a = a$ | $a+b = 0$ and $b+a = 0$]

(B): [select: | $((a+b)+c) \bmod m$ | $(a+(b+c)) \bmod m$ | $(a+b) \bmod m$ | $(b+a) \bmod m$ | $(a(b+c)) \bmod m$ | $(ab+ac) \bmod m$]

(C): [select: | $((a+b)+c) \bmod m$ | $(a+(b+c)) \bmod m$ | $(a+b) \bmod m$ | $(b+a) \bmod m$ | $(a(b+c)) \bmod m$ | $(ab+ac) \bmod m$]

Hence the operation $\oplus$ is ____.

[select: | **associative** | **commutative** | **disruptive** | **distributive** | **orderly**]

We have shown that

- (a) the set S contains an identity with respect to the operation $\oplus$,
- (b) for each element in S the set S contains an inverse with respect to $\oplus$,
- (c) the operation $\oplus$ is associative,
- (d) the operation $\oplus$ is commutative.

Thus the set S with the operation $\oplus$ is a commutative group.

Solutions

Problem 14.4 (1) *Correct Answers:*

- 0
- 0
- 2
- 0
- 3
- 0
- 1
- 2
- the identity element is 0
- 0
- 3
- 2
- 1
- each element has an inverse
- commutative
- a commutative group

Problem 14.4 (2) *Correct Answers:*

- 8
- 11
- 15
- 16

Problem 14.4 (3) *Correct Answers:*

- a
- a
- 0
- identity
- $m-a$
- $m-a$
- inverse
- $(a+b)+c = a+(b+c)$
- $((a+b)+c) \bmod m$
- $(a+(b+c)) \bmod m$
- associative
- $a+b = b+a$
- $(a+b) \bmod m$
- $(b+a) \bmod m$
- commutative

14.5 Multiplicative Groups

Problem 14.5 (1) (1 point)

Fill in the operation table for the binary operation $\otimes$ on the set $\mathbb{Z}_7^\otimes$ defined by $a \otimes b = (a \cdot b) \bmod 7$:

$\otimes$	1	2	3	4	5	6
1	—	—	3	4	5	—
2	—	—	—	—	—	5
3	3	—	—	5	1	—
4	—	1	—	2	6	3
5	—	—	1	6	—	—
6	—	5	—	3	2	—

Complete the following:

(1) in $\mathbb{Z}_7^\otimes$ with respect to $\otimes$ ____.

[select: | **the identity element is 1** | **there is no identity element**]

(2) Find the inverses of the elements of $\mathbb{Z}_7^\otimes$ with respect to $\otimes$. If an element does not have an inverse answer 'none'.

The inverse of 1 is ____.

The inverse of 2 is ____.

The inverse of 3 is ____.

The inverse of 4 is ____.

The inverse of 5 is ____.

The inverse of 6 is ____.

With respect to $\otimes$ ____.

[select: | **each element has an inverse** | **at least one element does not have an inverse** | **there is no identity, so inverses are not defined**]

(3) $\otimes$ is associative.

(4) $\otimes$ is ____.

[select: | **commutative** | **not commutative**]

Decide whether $(\mathbb{Z}_7^\otimes, \otimes)$ is a commutative group:

The set $\mathbb{Z}_7^\otimes$ with the operation $\otimes$ is ____.

[select: | **a commutative group** | **not a commutative group**]

Problem 14.5 (2) (1 point)

Find the inverses of the elements of $\mathbb{Z}_{20}$ with respect to

$\oplus : \mathbb{Z}_{20} \times \mathbb{Z}_{20} \rightarrow \mathbb{Z}_{20}$ defined by $a \oplus b = a + b \bmod 20$.

The inverse of 0 is ____.

The inverse of 12 is ____.

The inverse of 3 is ____.

The inverse of 13 is ____.

Problem 14.5 (3) (1 point)

In the group $(\mathbb{Z}_{19}^\otimes, \otimes)$ where $a \otimes b = (a \cdot b) \bmod 19$ find the inverse of 6 with respect to $\otimes$. Fill in the blanks.

(1) We have $\gcd(19, 6) =$ ____.

(2) By Bezout's identity there are integers s and t such that $s \cdot 19 + t \cdot 6 = \gcd(19, 6)$.

We have ____ $\cdot 19 +$ ____ $\cdot 6 = \gcd(19, 6) =$ ____.

(3) The inverse of 6 in $\mathbb{Z}_{19}^\otimes$ with respect to $\otimes$ is ____.

Problem 14.5 (4) (1 point)

In the group $(\mathbb{Z}_{13}^\otimes, \otimes)$ where $a \otimes b = (a \cdot b) \bmod 13$ find the inverse of 4 with respect to $\otimes$. Fill in the blanks.

(1) We have $\gcd(13, 4) =$ ____.

(2) By Bezout's identity there are integers s and t such that $s \cdot 13 + t \cdot 4 = \gcd(13, 4)$.

We have ____ $\cdot 13 +$ ____ $\cdot 4 = \gcd(13, 4) =$ ____.

(3) The inverse of 4 in $\mathbb{Z}_{13}^\otimes$ with respect to $\otimes$ is ____.

Problem 14.5 (5) (1 point)

Find the inverses of the elements of $\mathbb{Z}_3^\otimes$ with respect to

$\otimes : \mathbb{Z}_3^\otimes \times \mathbb{Z}_3^\otimes \rightarrow \mathbb{Z}_3^\otimes$ defined by $a \otimes b = a \cdot b \bmod 3$.

The inverse of 1 is ____.

The inverse of 2 is ____.

Problem 14.5 (6) (1 point)

Let p be a prime number. Let $S=1,2,3,\dots,p-1$. Let $\otimes:S\times S\rightarrow S$ be given by $a\otimes b=(a\cdot b) \bmod p$.

We show that $(S,\otimes)$ is a group.

(a) Because $a\otimes 1 = \underline{\text{(A)}}$ and $1\otimes a = \underline{\text{(B)}}$ for all a in S , the element $\underline{\text{(C)}}$ is the $\underline{\text{(D)}}$ with respect to the operation $\otimes$.

(A): [select: | **a** | **p** | **s** | **t** | **0** | **1**]

(B): [select: | **a** | **p** | **s** | **t** | **0** | **1**]

(C): [select: | **a** | **p** | **s** | **t** | **0** | **1**]

(D): [select: | **analogue** | **identity** | **inverse** | **opposite** | **unit**]

(b) Let a in $1,2,3,\dots,p-1$. As p is prime we have $\gcd(a,p) = \underline{\text{(A)}}$.
By Bezout's theorem there are integers s and t such that $s\cdot a+t\cdot p = \underline{\text{(B)}}$.
Thus $\underline{\text{(C)}} \otimes a = (\underline{\text{(D)}} \cdot a) \bmod p = 1$.
So $\underline{\text{(E)}} \bmod p$ is the $\underline{\text{(F)}}$ of a with respect to $\otimes$.

(A): [select: | **a** | **p** | **s** | **t** | **0** | **1**]

(B): [select: | **a** | **p** | **s** | **t** | **0** | **1**]

(C): [select: | **a** | **p** | **s** | **t** | **0** | **1**]

(D): [select: | **a** | **p** | **s** | **t** | **0** | **1**]

(E): [select: | **a** | **p** | **s** | **t** | **0** | **1**]

(F): [select: | **analogue** | **identity** | **inverse** | **opposite** | **unit**]

(c) The multiplication of integers is _____, that is, $(a\cdot b)\cdot c = a\cdot(b\cdot c)$ for all integers a , b , and c . Thus for all a , b , and c in S we have $(a\otimes b)\otimes c = ((a\cdot b)\cdot c) \bmod p = (a\cdot(b\cdot c)) \bmod p = a\otimes(b\otimes c)$.

[select: | **associative** | **commutative** | **disruptive** | **distributive** | **negative** | **orderly** | **positive** |

transitive]

Hence the operation $\otimes$ is _____.

[select: | **associative** | **commutative** | **disruptive** | **distributive** | **negative** | **orderly** | **positive** | **transitive**]

(d) The multiplication of integers is _____, that is, $a \cdot b = b \cdot a$ for all integers a and b . Thus for all a and b in S we have $a \otimes b = (a \cdot b) \bmod p = (b \cdot a) \bmod p = b \otimes a$.

[select: | **associative** | **commutative** | **disruptive** | **distributive** | **negative** | **orderly** | **positive** | **transitive**]

Hence the operation $\otimes$ is _____.

[select: | **associative** | **commutative** | **disruptive** | **distributive** | **negative** | **orderly** | **positive** | **transitive**]

We have shown that

(a) the set S contains an _____ with respect to the operation $\otimes$,

[select: | **analogue** | **identity** | **inverse** | **opposite** | **unit**]

(b) for each element in S the set S contains an _____ with respect to $\otimes$,

[select: | **analogue** | **identity** | **inverse** | **opposite** | **unit**]

(c) the operation $\otimes$ is associative,

(d) the operation $\otimes$ is _____.

[select: | **associative** | **commutative** | **disruptive** | **distributive** | **negative** | **orderly** | **positive** | **transitive**]

Thus the set S with the operation $\otimes$ is a commutative group.

Solutions

Problem 14.5 (1) *Correct Answers:*

- 1
- 2
- 6
- 2
- 4
- 6
- 1
- 3
- 6
- 2
- 4
- 4
- 5
- 5
- 3
- 4
- 2
- 6
- 4
- 1
- the identity element is 1
- 1
- 4
- 5
- 2
- 3
- 6
- each element has an inverse
- commutative
- a commutative group

Problem 14.5 (2) *Correct Answers:*

- 0
- 8
- 17
- 7

Problem 14.5 (3) *Correct Answers:*

Hint: (2) Let a and b be natural numbers. If $\gcd(a, b) = a \bmod b$ then $s \cdot a + t \cdot b = \gcd(a, b)$ for $s = 1$ and $t = -(a \operatorname{div} b)$.

(3) $b \in \mathbb{Z}_{19}^{\otimes}$ is the inverse of 6 when $b \otimes 6 = (b \cdot 6) \bmod 19 = 1$.

Correct Answers:

- 1
- $-3; 1$
- 1
- 16

Problem 14.5 (4) *Correct Answers:*

Hint: (2) Let a and b be natural numbers. If $\gcd(a, b) = a \bmod b$ then $s \cdot a + t \cdot b = \gcd(a, b)$ for $s = 1$ and $t = -(a \operatorname{div} b)$.

(3) $b \in \mathbb{Z}_{13}^{\otimes}$ is the inverse of 4 when $b \otimes 4 = (b \cdot 4) \bmod 13 = 1$.

Correct Answers:

- 1
- $-3; 1$
- 1
- 10

Problem 14.5 (5) *Correct Answers:*

- 1
- 2

Problem 14.5 (6) *Correct Answers:*

- a
- a
- 1
- identity
- 1
- 1
- s
- s
- s
- inverse
- associative
- associative
- commutative
- commutative
- identity
- inverse
- commutative

Chapter 15

Powers and Logarithms

1. Exponentiation
2. Repeated Squaring
3. Fast Exponentiation
4. Discrete Logarithm

15.1 Exponentiation

Problem 15.1 (1) (1 point)

In $(\mathbb{Z}_5^\otimes, \otimes)$ where $a \otimes b = (a \cdot b) \bmod 5$ compute:

$$4^{0\otimes} = \underline{\hspace{1cm}}$$

$$4^{1\otimes} = \underline{\hspace{1cm}}$$

$$4^{2\otimes} = \underline{\hspace{1cm}}$$

$$4^{3\otimes} = \underline{\hspace{1cm}}$$

$$4^{4\otimes} = \underline{\hspace{1cm}}$$

Use the information above to find the smallest non-negative integer n such that $4^{n\otimes} = 1$.

$$n = \underline{\hspace{1cm}}$$

Problem 15.1 (2) (1 point)

In $(\mathbb{Z}_7^\otimes, \otimes)$ where $a \otimes b := (a \cdot b) \bmod 7$ compute:

$$5^{0\otimes} = \underline{\hspace{1cm}}$$

$$5^{1\otimes} = \underline{\hspace{1cm}}$$

$$5^{2\otimes} = \underline{\hspace{1cm}}$$

$$5^{3\otimes} = \underline{\hspace{1cm}}$$

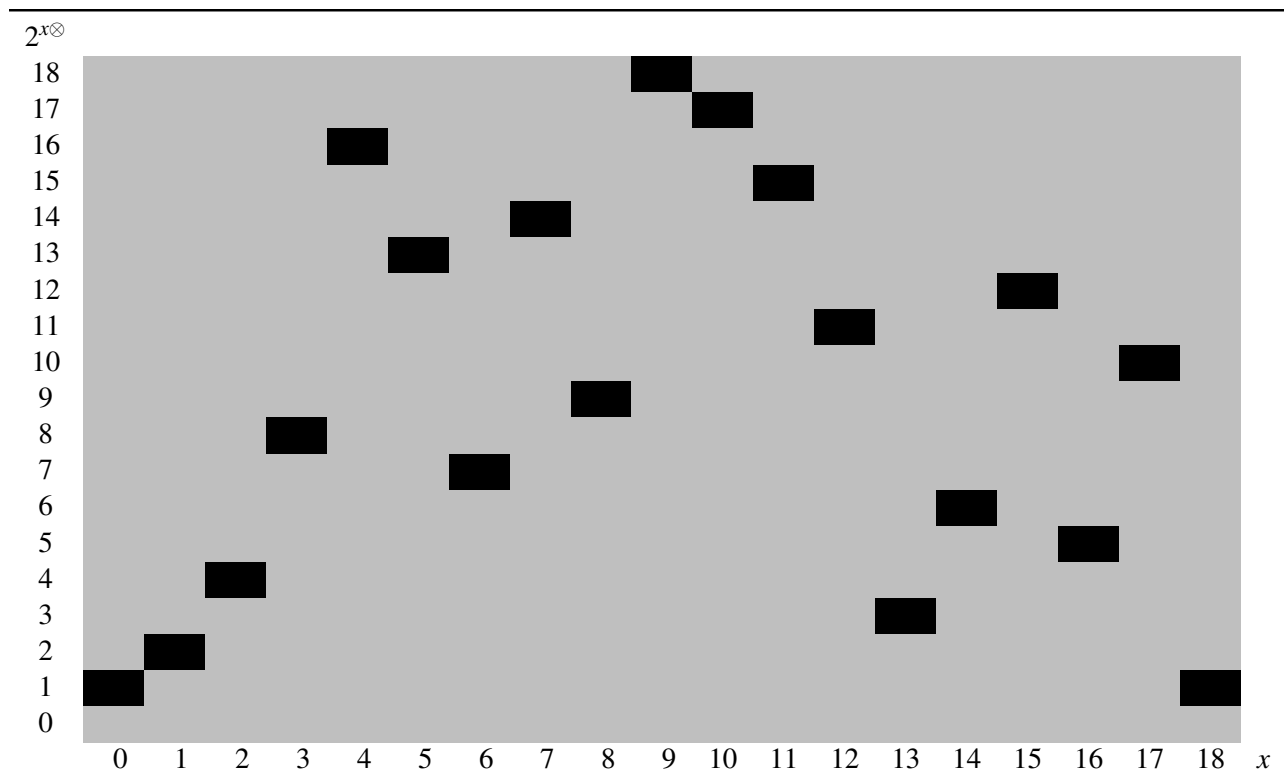
$$5^{4\otimes} = \underline{\hspace{1cm}}$$

$$5^{5\otimes} = \underline{\hspace{1cm}}$$

$$5^{6\otimes} = \underline{\hspace{1cm}}$$

Problem 15.1 (3) (1 point)

We consider the function $h : \mathbb{Z}_{19} \rightarrow \mathbb{Z}_{19}$ given by $h(x) = 2^{x\otimes} = 2^x \bmod 19$.



Find the following:

$$2^{0\otimes} = \underline{\hspace{1cm}}$$

$$2^{3\otimes} = \underline{\hspace{1cm}}$$

$$2^{5\otimes} = \underline{\hspace{1cm}}$$

$$2^{7\otimes} = \underline{\hspace{1cm}}$$

$$2^{8\otimes} = \underline{\hspace{1cm}}$$

$$2^{9\otimes} = \underline{\hspace{1cm}}$$

$$2^{11\otimes} = \underline{\hspace{1cm}}$$

$$2^{14\otimes} = \underline{\hspace{1cm}}$$

$$2^{18\otimes} = \underline{\hspace{1cm}}$$

Problem 15.1 (4) (1 point)

Let $(G, \otimes)$ be a group and $b \in G$. We set $b^{0\otimes} = e$ where $e \in G$ is the identity of $(G, \otimes)$. For $n \in \mathbb{N}$ we set

$$b^{n\otimes} = \underbrace{b \otimes b \otimes \cdots \otimes b}_{n \text{ times}}.$$

In $(\mathbb{Z}_{17}^{\otimes}, \otimes)$ where $a \otimes b = (a \cdot b) \bmod 17$ compute:

$$1^{2\otimes} = \underline{\hspace{1cm}}$$

$$2^{4\otimes} = \underline{\hspace{1cm}}$$

$$4^{2\otimes} = \underline{\hspace{1cm}}$$

$$5^{2\otimes} = \underline{\hspace{1cm}}$$

Problem 15.1 (5) (1 point)

Let p be a prime number. Consider the following in the group $(\mathbb{Z}_p^{\otimes}, \otimes)$ where $a \otimes b := (a \cdot b) \bmod p$.

Match the expressions that are equal for all $a \in \mathbb{Z}_p^{\otimes}$ and all non-negative integers n by entering the letters next to the numbers.

- | | |
|--|--|
| <u> </u> 1. $a^{3\otimes}$ | A. $a^{2\otimes}$ |
| <u> </u> 2. $a^{(n+m)\otimes}$ | B. a |
| <u> </u> 3. $a^{1\otimes}$ | C. $a^{n\otimes} \otimes a^{m\otimes}$ |
| <u> </u> 4. $(a^{n\otimes})^{m\otimes}$ | D. $a^{(n \cdot m)\otimes}$ |
| <u> </u> 5. $a \otimes a$ | E. 1 |
| <u> </u> 6. $a^{0\otimes}$ | F. $a \otimes a \otimes a$ |

Problem 15.1 (6) (1 point)

Naive Exponentiation

With the naive exponentiation algorithm find $3^{15} \bmod 19$.

Input: Base $b := \underline{\hspace{1cm}}$ an exponent $n := \underline{\hspace{1cm}}$ and a modulus $m := \underline{\hspace{1cm}}$.

let $c := 3$ and **let** $i := 1$.

let $c := (c \cdot 3) \bmod 19 = \underline{\hspace{1cm}}$ and **let** $i := i + 1 = \underline{\hspace{1cm}}$

let $c := (c \cdot 3) \bmod 19 = \underline{\hspace{1cm}}$ and **let** $i := i + 1 = \underline{\hspace{1cm}}$

let $c := (c \cdot 3) \bmod 19 = \underline{\hspace{1cm}}$ and **let** $i := i + 1 = \underline{\hspace{1cm}}$

let $c := (c \cdot 3) \bmod 19 = \underline{\hspace{1cm}}$ and **let** $i := i + 1 = \underline{\hspace{1cm}}$

let $c := (c \cdot 3) \bmod 19 = \underline{\hspace{1cm}}$ and **let** $i := i + 1 = \underline{\hspace{1cm}}$

let $c := (c \cdot 3) \bmod 19 = \underline{\hspace{1cm}}$ and **let** $i := i + 1 = \underline{\hspace{1cm}}$

let $c := (c \cdot 3) \bmod 19 = \underline{\hspace{1cm}}$ and **let** $i := i + 1 = \underline{\hspace{1cm}}$

let $c := (c \cdot 3) \bmod 19 = \underline{\hspace{1cm}}$ and **let** $i := i + 1 = \underline{\hspace{1cm}}$

let $c := (c \cdot 3) \bmod 19 = \underline{\hspace{1cm}}$ and **let** $i := i + 1 = \underline{\hspace{1cm}}$

let $c := (c \cdot 3) \bmod 19 = \underline{\hspace{1cm}}$ and **let** $i := i + 1 = \underline{\hspace{1cm}}$

let $c := (c \cdot 3) \bmod 19 = \underline{\hspace{1cm}}$ and **let** $i := i + 1 = \underline{\hspace{1cm}}$

let $c := (c \cdot 3) \bmod 19 = \underline{\hspace{1cm}}$ and **let** $i := i + 1 = \underline{\hspace{1cm}}$

let $c := (c \cdot 3) \bmod 19 = \underline{\hspace{1cm}}$ and **let** $i := i + 1 = \underline{\hspace{1cm}}$

let $c := (c \cdot 3) \bmod 19 = \underline{\hspace{1cm}}$ and **let** $i := i + 1 = \underline{\hspace{1cm}}$

Because the statement $i = 15$ is true, the loop ends here.

Output: $3^{15} \bmod 19 = c = \underline{\hspace{1cm}}$.

Problem 15.1 (7) (1 point)

In $(\mathbb{Z}_{13}^{\otimes}, \otimes)$ where $a \otimes b := (a \cdot b) \bmod 13$ compute:

$$3^{0\otimes} = \underline{\hspace{1cm}}$$

$$3^{1\otimes} = \underline{\hspace{1cm}}$$

$$3^{2\otimes} = 3^{(1+1)\otimes} = 3^{1\otimes} \otimes 3 = __\otimes 3 = (__\cdot 3) \bmod 13 = __\$$

$$3^{3\otimes} = 3^{(2+1)\otimes} = 3^{2\otimes} \otimes 3 = __\otimes 3 = (__\cdot 3) \bmod 13 = __\$$

$$3^{4\otimes} = 3^{(3+1)\otimes} = 3^{3\otimes} \otimes 3 = __\otimes 3 = (__\cdot 3) \bmod 13 = __\$$

$$3^{5\otimes} = 3^{(4+1)\otimes} = 3^{4\otimes} \otimes 3 = __\otimes 3 = (__\cdot 3) \bmod 13 = __\$$

$$3^{6\otimes} = 3^{(5+1)\otimes} = 3^{5\otimes} \otimes 3 = __\otimes 3 = (__\cdot 3) \bmod 13 = __\$$

Solutions

Problem 15.1 (1) *Correct Answers:*

- 1
- 4
- 1
- 4
- 1
- 0

Problem 15.1 (2) *Correct Answers:*

Hint: Use that $5^{(n+m)\otimes} = 5^{n\otimes} \otimes 5^{m\otimes}$. For example, we have $5^{2\otimes} = 4$ and $5^{1\otimes} = 5$, thus

$$5^{3\otimes} = 5^{(2+1)\otimes} = 5^{2\otimes} \otimes 5 = 4 \otimes 5 = (4 \cdot 5) \bmod 7 = 6.$$

Correct Answers:

- 1
- 5
- 4
- 6
- 2
- 3
- 1

Problem 15.1 (3) *Correct Answers:*

Hint: The graph of the function $h : \mathbb{Z}_{19} \rightarrow \mathbb{Z}_{19}$ given by $h(x) = 2^{x\otimes} = 2^x \bmod 19$ is

$$\{(x, 2^x \bmod 19) \mid x \in \mathbb{Z}_{19}\} \subseteq \mathbb{Z}_{19} \times \mathbb{Z}_{19}$$

In the plot the elements of the graph are represented by black pixels.

Correct Answers:

- 1
- 8
- 13
- 14
- 9
- 18
- 15
- 6
- 1

Problem 15.1 (4) *Correct Answers:*

- 1
- 16
- 16
- 8

Problem 15.1 (5) *Correct Answers:*

- F
- C
- B
- D
- A
- E

Problem 15.1 (6) *Correct Answers:*

- 3
- 15
- 19
- 9
- 2
- 8
- 3
- 5
- 4
- 15
- 5
- 7
- 6
- 2
- 7
- 6
- 8
- 18
- 9
- 16
- 10
- 10
- 11
- 11
- 12
- 14
- 13
- 4
- 14
- 12
- 15
- 12

Problem 15.1 (7) *Correct Answers:*

Hint: We have $3^{2\otimes} = 9$ and $3^{1\otimes} = 3$, thus

$$3^{3\otimes} = 3^{(2+1)\otimes} = 3^{2\otimes} \otimes 3 = 9 \otimes 3 = (9 \cdot 3) \bmod 13 = 27 \bmod 13 = 1.$$

Correct Answers:

- 1
- 3
- 3
- 3
- 9
- 9
- 9
- 1
- 1
- 1
- 3
- 3
- 3
- 9
- 9
- 9
- 1

15.2 Repeated Squaring

Problem 15.2 (1) (1 point)

Let $(G, \otimes)$ be a group and $b \in G$. We set $b^{0\otimes} = e$ where $e \in G$ is the identity of $(G, \otimes)$. For $n \in \mathbb{N}$ we set

$$b^{n\otimes} = \underbrace{b \otimes b \otimes \cdots \otimes b}_{n \text{ copies of } b}.$$

In $(\mathbb{Z}_{41}^{\otimes}, \otimes)$ where $a \otimes b = (a \cdot b) \bmod 41$ follow these steps to compute $5^{32\otimes}$.

$$5^{1\otimes} = \underline{\hspace{1cm}}$$

$$5^{2\otimes} = 5^{1\otimes} \otimes 5^{1\otimes} = \underline{\hspace{1cm}} \otimes \underline{\hspace{1cm}} = \underline{\hspace{1cm}}$$

$$5^{4\otimes} = 5^{2\otimes} \otimes 5^{2\otimes} = \underline{\hspace{1cm}} \otimes \underline{\hspace{1cm}} = \underline{\hspace{1cm}}$$

$$5^{8\otimes} = 5^{4\otimes} \otimes 5^{4\otimes} = \underline{\hspace{1cm}} \otimes \underline{\hspace{1cm}} = \underline{\hspace{1cm}}$$

$$5^{16\otimes} = 5^{8\otimes} \otimes 5^{8\otimes} = \underline{\hspace{1cm}} \otimes \underline{\hspace{1cm}} = \underline{\hspace{1cm}}$$

$$5^{32\otimes} = 5^{16\otimes} \otimes 5^{16\otimes} = \underline{\hspace{1cm}} \otimes \underline{\hspace{1cm}} = \underline{\hspace{1cm}}$$

Problem 15.2 (2) (1 point)

Let p be a prime number. Consider the following in the group $(\mathbb{Z}_p^{\otimes}, \otimes)$ where $a \otimes b := (a \cdot b) \bmod p$.

Match the expressions that are equal for all $a \in \mathbb{Z}_p^{\otimes}$ and all non-negative integers n by entering the letters next to the numbers.

- | | |
|----------------------------------|--|
| ___ 1. $a^{64 \otimes}$ | A. $a^{4 \otimes} \otimes a^{4 \otimes}$ |
| ___ 2. $a^{8 \otimes}$ | B. $a^{n \otimes} \otimes a^{n \otimes}$ |
| ___ 3. $a^{128 \otimes}$ | C. $a^{16 \otimes} \otimes a^{16 \otimes}$ |
| ___ 4. $a^{2 \otimes}$ | D. $a^{64 \otimes} \otimes a^{64 \otimes}$ |
| ___ 5. $a^{4 \otimes}$ | E. $a^{32 \otimes} \otimes a^{32 \otimes}$ |
| ___ 6. $a^{32 \otimes}$ | F. $a \otimes a$ |
| ___ 7. $a^{(2 \cdot n) \otimes}$ | G. $a^{2 \otimes} \otimes a^{2 \otimes}$ |
| ___ 8. $a^{16 \otimes}$ | H. $a^{8 \otimes} \otimes a^{8 \otimes}$ |

Problem 15.2 (3) (1 point)

Let $\otimes : \mathbb{Z}_{19937}^{\otimes} \times \mathbb{Z}_{19937}^{\otimes} \rightarrow \mathbb{Z}_{19937}^{\otimes}$ be the binary operation given by $a \otimes b = (a \cdot b) \bmod 19937$.

We set $b^{0 \otimes} := e$ where $e \in G$ is the identity of $(G, \otimes)$. For $n \in \mathbb{N}$ we set

$$b^{n \otimes} := \underbrace{b \otimes b \otimes \cdots \otimes b}_{n \text{ copies of } b}.$$

How many operations $\otimes$ are needed to compute $3^{8 \otimes}$ with the **naïve** exponentiation method (repeated multiplication by 3) ?

How many operations $\otimes$ are needed to compute $3^{8 \otimes}$ with the **repeated squaring** method ?

Problem 15.2 (4) (1 point)

There are many methods to calculate $x^{(2^k)}$ for some positive integer k and given x .

Naïve Exponentiation

The first naïve method, just multiplies x with itself to find x^2 and then multiplies x with x^2 to find x^3 and keeps going like this till x^{2^k} is found.

Problem 15.2 (6) (1 point)

Let $(G, \otimes)$ be a group and $b \in G$. We set $b^{0\otimes} = e$ where $e \in G$ is the identity of $(G, \otimes)$. For $n \in \mathbb{N}$ we set

$$b^{n\otimes} = \underbrace{b \otimes b \otimes \cdots \otimes b}_{n \text{ copies of } b}.$$

In $(\mathbb{Z}_{83}^{\otimes}, \otimes)$ where $a \otimes b = (a \cdot b) \bmod 83$ follow these steps to compute $5^{32\otimes}$.

$$5^{1\otimes} = \underline{\hspace{1cm}}$$

$$5^{2\otimes} = 5^{1\otimes} \otimes 5^{1\otimes} = \underline{\hspace{1cm}} \otimes \underline{\hspace{1cm}} = \underline{\hspace{1cm}}$$

$$5^{4\otimes} = 5^{2\otimes} \otimes 5^{2\otimes} = \underline{\hspace{1cm}} \otimes \underline{\hspace{1cm}} = \underline{\hspace{1cm}}$$

$$5^{8\otimes} = 5^{4\otimes} \otimes 5^{4\otimes} = \underline{\hspace{1cm}} \otimes \underline{\hspace{1cm}} = \underline{\hspace{1cm}}$$

$$5^{16\otimes} = 5^{8\otimes} \otimes 5^{8\otimes} = \underline{\hspace{1cm}} \otimes \underline{\hspace{1cm}} = \underline{\hspace{1cm}}$$

$$5^{32\otimes} = 5^{16\otimes} \otimes 5^{16\otimes} = \underline{\hspace{1cm}} \otimes \underline{\hspace{1cm}} = \underline{\hspace{1cm}}$$

Problem 15.2 (7) (1 point)

Let $(G, \otimes)$ be a group and $b \in G$. We set $b^{0\otimes} = e$ where $e \in G$ is the identity of $(G, \otimes)$. For $n \in \mathbb{N}$ we set

$$b^{n\otimes} = \underbrace{b \otimes b \otimes \cdots \otimes b}_{n \text{ copies of } b}.$$

In $(\mathbb{Z}_{79}^{\otimes}, \otimes)$ where $a \otimes b = (a \cdot b) \bmod 79$ we have

$$5^{16\otimes} = 31.$$

Compute

$$5^{32\otimes} = 5^{16\otimes} \otimes 5^{16\otimes} = \underline{\hspace{1cm}} \otimes \underline{\hspace{1cm}} = \underline{\hspace{1cm}}$$

Problem 15.2 (8) (1 point)

Let $(G, \otimes)$ be a group and $b \in G$. We set $b^{0\otimes} = e$ where $e \in G$ is the identity of $(G, \otimes)$. For $n \in \mathbb{N}$ we set

$$b^{n\otimes} = \underbrace{b \otimes b \otimes \cdots \otimes b}_{n \text{ copies of } b}.$$

In $(\mathbb{Z}_{103}^\otimes, \otimes)$ where $a \otimes b = (a \cdot b) \bmod 103$ follow these steps to compute $15^{64\otimes}$.

$$15^{1\otimes} = \underline{\hspace{2cm}}$$

$$15^{2\otimes} = \underline{\hspace{2cm}}$$

$$15^{4\otimes} = \underline{\hspace{2cm}}$$

$$15^{8\otimes} = \underline{\hspace{2cm}}$$

$$15^{16\otimes} = \underline{\hspace{2cm}}$$

$$15^{32\otimes} = \underline{\hspace{2cm}}$$

$$15^{64\otimes} = \underline{\hspace{2cm}}$$

Solutions

Problem 15.2 (1) *Correct Answers:*

Hint: We have $b^{n\otimes} = b^n \bmod 41$. Always compute $\bmod 41$ before entering the answers.

Correct Answers:

- 5
- 5
- 5
- 25
- 25
- 25
- 10
- 10
- 10
- 18
- 18
- 18
- 37
- 37
- 37
- 16

Problem 15.2 (2) *Correct Answers:*

- E
- A
- D
- F
- G
- C
- B
- H

Problem 15.2 (3) *Correct Answers:*

Hint: $8 = 2^3$

Correct Answers:

- 7
- 3

Problem 15.2 (4) *Correct Answers:*

Hint: $128 = 2^7$.

Correct Answers:

- 127
- 7
- B

Problem 15.2 (5) *Correct Answers:*

- 36
- 36
- 51

Problem 15.2 (6) *Correct Answers:*

Hint: We have $b^{n\otimes} = b^n \bmod 83$. Always compute $\bmod 83$ before entering the answers.

Correct Answers:

- 5
- 5
- 5
- 25
- 25
- 25
- 44
- 44
- 44
- 27
- 27
- 27
- 65
- 65
- 65
- 75

Problem 15.2 (7) *Correct Answers:*

- 31
- 31
- 13

Problem 15.2 (8) *Correct Answers:*

Hint: Use that for all natural numbers m we have $15^{(2m)\otimes} = 15^{(m+m)\otimes} = 15^{m\otimes} \otimes 15^{m\otimes}$.

Correct Answers:

- 15
- 19
- 52
- 26
- 58
- 68
- 92

15.3 Fast Exponentiation

Problem 15.3 (1) (1 point)

You are given the following information:

(1) These powers of 2 modulo 181 can be computed using repeated squaring:

$$2^1 \bmod 181 = 2$$

$$2^2 \bmod 181 = 4$$

$$2^4 \bmod 181 = 16$$

$$2^8 \bmod 181 = 75$$

$$2^{16} \bmod 181 = 14$$

$$2^{32} \bmod 181 = 15$$

$$2^{64} \bmod 181 = 44$$

(2) We have $18 = 2 + 16$

Now compute:

$$2^{18} \bmod 181 = \underline{\hspace{2cm}}$$

Problem 15.3 (2) (1 point)

These powers of 6 modulo 251 can be computed using repeated squaring:

$$6^1 \bmod 251 = 6$$

$$6^2 \bmod 251 = 36$$

$$6^4 \bmod 251 = 41$$

$$6^8 \bmod 251 = 175$$

$$6^{16} \bmod 251 = 3$$

Now compute:

$$6^6 \bmod 251 = \underline{\hspace{2cm}}$$

Problem 15.3 (3) (1 point)

Fast Exponentiation

With the fast exponentiation algorithm find $4^8 \bmod 19$.

Input: Base $b := \underline{\hspace{1cm}}$ an exponent $n := \underline{\hspace{1cm}}$ and a modulus $m := \underline{\hspace{1cm}}$.

let $a := 1$ and **let** $c := b = \underline{\hspace{1cm}}$.

let $r := n \bmod 2 = \underline{\hspace{1cm}}$. **if** $r = 1$ **then let** $a := (a \cdot c) \bmod 19$. Now $a = \underline{\hspace{1cm}}$

let $n := n \div 2 = \underline{\hspace{1cm}}$

and **let** $c := (c \cdot c) \bmod 19 = \underline{\hspace{1cm}}$

let $r := n \bmod 2 = \underline{\hspace{1cm}}$. **if** $r = 1$ **then let** $a := (a \cdot c) \bmod 19$. Now $a = \underline{\hspace{1cm}}$

let $n := n \div 2 = \underline{\hspace{1cm}}$

and **let** $c := (c \cdot c) \bmod 19 = \underline{\hspace{1cm}}$

let $r := n \bmod 2 = \underline{\hspace{1cm}}$. **if** $r = 1$ **then let** $a := (a \cdot c) \bmod 19$. Now $a = \underline{\hspace{1cm}}$

let $n := n \div 2 = \underline{\hspace{1cm}}$

and **let** $c := (c \cdot c) \bmod 19 = \underline{\hspace{1cm}}$

let $r := n \bmod 2 = \underline{\hspace{1cm}}$. **if** $r = 1$ **then let** $a := (a \cdot c) \bmod 19$. Now $a = \underline{\hspace{1cm}}$

let $n := n \div 2 = \underline{\hspace{1cm}}$

Because the statement $n = 0$ is true, the loop ends here.

Output: $4^8 \bmod 19 = a = \underline{\hspace{1cm}}$.

Problem 15.3 (4) (1 point)

Let $\otimes : \mathbb{Z}_{41}^{\otimes} \times \mathbb{Z}_{41}^{\otimes} \rightarrow \mathbb{Z}_{41}^{\otimes}$ be given by $a \otimes b = (a \cdot b) \bmod 41$. We compute

$$9^{48\otimes} = \underbrace{9 \otimes 9 \otimes \cdots \otimes 9}_{48 \text{ times}} = 9^{48} \bmod 41$$

using fast exponentiation.

Find the base 2 expansion of 48.

$$48 = (\underline{\hspace{1cm}} \cdot 64) + (\underline{\hspace{1cm}} \cdot 32) + (\underline{\hspace{1cm}} \cdot 16) + (\underline{\hspace{1cm}} \cdot 8) + (\underline{\hspace{1cm}} \cdot 4) + (\underline{\hspace{1cm}} \cdot 2) + (\underline{\hspace{1cm}} \cdot 1)$$

Complete the table. In the right column decide whether the power of 9 occurs in the product evaluated to find $9^{48\otimes}$ when using fast exponentiation.

$9^{1\otimes} = \underline{\hspace{1cm}}$	[select: yes no]
$9^{2\otimes} = 9^{1\otimes} \otimes 9^{1\otimes} = \underline{\hspace{1cm}}$	[select: yes no]
$9^{4\otimes} = 9^{2\otimes} \otimes 9^{2\otimes} = \underline{\hspace{1cm}}$	[select: yes no]
$9^{8\otimes} = 9^{4\otimes} \otimes 9^{4\otimes} = \underline{\hspace{1cm}}$	[select: yes no]
$9^{16\otimes} = 9^{8\otimes} \otimes 9^{8\otimes} = \underline{\hspace{1cm}}$	[select: yes no]
$9^{32\otimes} = 9^{16\otimes} \otimes 9^{16\otimes} = \underline{\hspace{1cm}}$	[select: yes no]
$9^{64\otimes} = 9^{32\otimes} \otimes 9^{32\otimes} = \underline{\hspace{1cm}}$	[select: yes no]

Use these values to compute $9^{48\otimes}$

$$9^{48\otimes} = \underline{\hspace{1cm}}$$

Problem 15.3 (5) (1 point)

Let $\otimes : \mathbb{Z}_{11}^{\otimes} \times \mathbb{Z}_{11}^{\otimes} \rightarrow \mathbb{Z}_{11}^{\otimes}$ be given by $a \otimes b = (a \cdot b) \bmod 11$. Compute

$$5^{4\otimes} = \underbrace{5 \otimes 5 \otimes \cdots \otimes 5}_{4 \text{ times}} = 5^4 \bmod 11$$

using fast exponentiation.

Find the base 2 expansion of 4.

$$4 = (\underline{\hspace{1cm}} \cdot 16) + (\underline{\hspace{1cm}} \cdot 8) + (\underline{\hspace{1cm}} \cdot 4) + (\underline{\hspace{1cm}} \cdot 2) + (\underline{\hspace{1cm}} \cdot 1)$$

Complete the table. In the right column decide whether the power of 5 occurs in the product that is used to find $5^{4\otimes}$ when using fast exponentiation.

$$5^{1\otimes} = \underline{\hspace{2cm}} \quad \text{[select: | yes | no]}$$

$$5^{2\otimes} = 5^{1\otimes} \otimes 5^{1\otimes} = \underline{\hspace{2cm}} \quad \text{[select: | yes | no]}$$

$$5^{4\otimes} = 5^{2\otimes} \otimes 5^{2\otimes} = \underline{\hspace{2cm}} \quad \text{[select: | yes | no]}$$

$$5^{8\otimes} = 5^{4\otimes} \otimes 5^{4\otimes} = \underline{\hspace{2cm}} \quad \text{[select: | yes | no]}$$

$$5^{16\otimes} = 5^{8\otimes} \otimes 5^{8\otimes} = \underline{\hspace{2cm}} \quad \text{[select: | yes | no]}$$

Use the above to compute $5^{4\otimes}$

$$5^{4\otimes} = \underline{\hspace{2cm}}$$

Problem 15.3 (6) (1 point)

Let $\otimes : \mathbb{Z}_{37}^{\otimes} \times \mathbb{Z}_{37}^{\otimes} \rightarrow \mathbb{Z}_{37}^{\otimes}$ be given by $a \otimes b = (a \cdot b) \bmod 37$. Compute

$$7^{15\otimes} = \underbrace{7 \otimes \cdots \otimes 7}_{15 \text{ copies of } 7} = 7^{15} \bmod 37.$$

using that $7^{1\otimes} = 7$, $7^{2\otimes} = 12$, $7^{4\otimes} = 33$, $7^{8\otimes} = 16$.

$$7^{15\otimes} = \underline{\hspace{2cm}}$$

Problem 15.3 (7) (1 point)

Let $\otimes : \mathbb{Z}_{1087}^{\otimes} \times \mathbb{Z}_{1087}^{\otimes} \rightarrow \mathbb{Z}_{1087}^{\otimes}$ be given by $a \otimes b = (a \cdot b) \bmod 1087$.

We have

$$3^{1\otimes} = 3, 3^{2\otimes} = 9, 3^{4\otimes} = 81, 3^{8\otimes} = 39, 3^{16\otimes} = 434, 3^{32\otimes} = 305$$

Use the above to compute:

$$3^{56\otimes} = \underbrace{3 \otimes \cdots \otimes 3}_{56 \text{ copies of } 3} = 3^{56} \bmod 1087.$$

$$3^{56\otimes} = \underline{\hspace{2cm}}$$

If the numbers become top big, compute " mod 1087 " after every multiplication.

Problem 15.3 (8) (1 point)

Let $\otimes : \mathbb{Z}_{73}^{\otimes} \times \mathbb{Z}_{73}^{\otimes} \rightarrow \mathbb{Z}_{73}^{\otimes}$ be given by $a \otimes b = (a \cdot b) \bmod 73$. Compute

$$7^{33\otimes} = \underbrace{7 \otimes 7 \otimes \cdots \otimes 7}_{33 \text{ times}} = 7^{33} \bmod 73$$

using fast exponentiation.

Complete the table. In the right column decide whether the power of 7 occurs in the product evaluated to find $7^{33\otimes}$ when using fast exponentiation.

$7^{1\otimes} = 7$	[select: yes no]
$7^{2\otimes} = 49$	[select: yes no]
$7^{4\otimes} = 65$	[select: yes no]
$7^{8\otimes} = 64$	[select: yes no]
$7^{16\otimes} = 8$	[select: yes no]
$7^{32\otimes} = 64$	[select: yes no]

Use these values to compute $7^{33\otimes}$

$$7^{33\otimes} = \underline{\hspace{2cm}}$$

Problem 15.3 (9) (1 point)

Let $\otimes : \mathbb{Z}_{23}^{\otimes} \times \mathbb{Z}_{23}^{\otimes} \rightarrow \mathbb{Z}_{23}^{\otimes}$ be given by $a \otimes b = (a \cdot b) \bmod 23$. Compute

$$5^{33\otimes} = \underbrace{5 \otimes 5 \otimes \cdots \otimes 5}_{33 \text{ times}} = 5^{33} \bmod 23$$

using fast exponentiation.

Find the base 2 expansion of 33.

$$33 = (\underline{\hspace{1cm}} \cdot 64) + (\underline{\hspace{1cm}} \cdot 32) + (\underline{\hspace{1cm}} \cdot 16) + (\underline{\hspace{1cm}} \cdot 8) + (\underline{\hspace{1cm}} \cdot 4) + (\underline{\hspace{1cm}} \cdot 2) + (\underline{\hspace{1cm}} \cdot 1)$$

Complete the table. In the right column decide whether the power of 5 occurs in the product evaluated to find $5^{33\otimes}$ when using fast exponentiation.

$$5^{1\otimes} = 5 \quad [\text{select: } | \text{ yes } | \text{ no }]$$

$$5^{2\otimes} = 2 \quad [\text{select: } | \text{ yes } | \text{ no }]$$

$$5^{4\otimes} = 4 \quad [\text{select: } | \text{ yes } | \text{ no }]$$

$$5^{8\otimes} = 16 \quad [\text{select: } | \text{ yes } | \text{ no }]$$

$$5^{16\otimes} = 3 \quad [\text{select: } | \text{ yes } | \text{ no }]$$

$$5^{32\otimes} = 9 \quad [\text{select: } | \text{ yes } | \text{ no }]$$

$$5^{64\otimes} = 12 \quad [\text{select: } | \text{ yes } | \text{ no }]$$

Use the above to compute $5^{33\otimes}$.

$$5^{33\otimes} = \underline{\hspace{2cm}}$$

Solutions

Problem 15.3 (1) *Correct Answers:*

Hint: Use that for all natural numbers m and n we have

$$2^{(m+n)\otimes} = 2^{m\otimes} \otimes 2^{n\otimes}.$$

Correct Answers:

- 56

Problem 15.3 (2) *Correct Answers:*

Hint: We have $6 = 2 + 4$

Use that for all natural numbers m and n we have

$$6^{(m+n)\otimes} = 6^{m\otimes} \otimes 6^{n\otimes}.$$

Correct Answers:

- 221

Problem 15.3 (3) *Correct Answers:*

- 4
- 8
- 19
- 4
- 0
- 1
- 4
- 16
- 0
- 1
- 2
- 9
- 0
- 1
- 1
- 5
- 1
- 5
- 0
- 5

Problem 15.3 (4) *Correct Answers:*

- 0
- 1
- 1
- 0

- 0
- 0
- 0
- 9
- no
- 40
- no
- 1
- no
- 1
- no
- 1
- yes
- 1
- yes
- 1
- no
- 1

Problem 15.3 (5) *Correct Answers:*

- 0
- 0
- 1
- 0
- 0
- 5
- no
- 3
- no
- 9
- yes
- 4
- no
- 5
- no
- 9

Problem 15.3 (6) *Correct Answers:*

- 26

Problem 15.3 (7) *Correct Answers:*

Hint: We have

$$56 = 2^3 + 2^4 + 2^5 = 8 + 16 + 32.$$

Thus

$$3^{56 \otimes} = 3^8 \otimes 3^{16} \otimes 3^{32}.$$

Correct Answers:

- 267

Problem 15.3 (8) *Correct Answers:*

- yes
- no
- no
- no
- no
- yes
- 10

Problem 15.3 (9) *Correct Answers:*

- 0
- 1
- 0
- 0
- 0
- 0
- 1
- yes
- no
- no
- no
- no
- yes
- no
- 22

15.4 Discrete Logarithm

Problem 15.4 (1) (1 point)

In $(\mathbb{Z}_{13}^{\otimes}, \otimes)$ where $a \otimes b = (a \cdot b) \bmod 13$ compute:

$$4^{0\otimes} = \underline{\hspace{1cm}}$$

$$4^{1\otimes} = \underline{\hspace{1cm}}$$

$$4^{2\otimes} = \underline{\hspace{1cm}}$$

$$4^{3\otimes} = \underline{\hspace{1cm}}$$

$$4^{4\otimes} = \underline{\hspace{1cm}}$$

$$4^{5\otimes} = \underline{\hspace{1cm}}$$

$$4^{6\otimes} = \underline{\hspace{1cm}}$$

$$4^{7\otimes} = \underline{\hspace{1cm}}$$

$$4^{8\otimes} = \underline{\hspace{1cm}}$$

$$4^{9\otimes} = \underline{\hspace{1cm}}$$

$$4^{10\otimes} = \underline{\hspace{1cm}}$$

$$4^{11\otimes} = \underline{\hspace{1cm}}$$

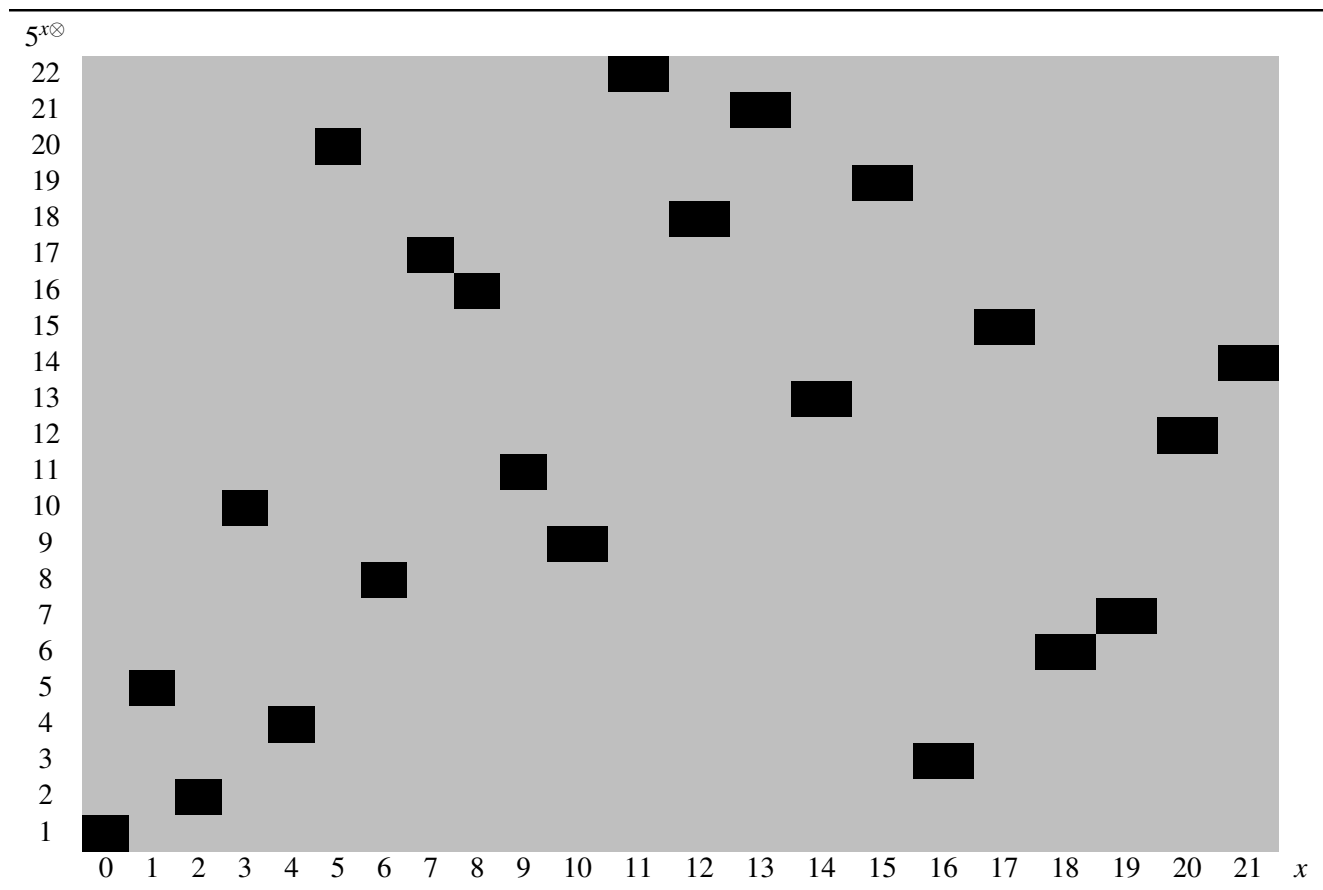
$$4^{12\otimes} = \underline{\hspace{1cm}}$$

Use the information above to find the smallest non-negative integer n such that $4^{n\otimes} = 1$.

$$n = \underline{\hspace{1cm}}$$

Problem 15.4 (2) (1 point)

Consider the function $g : \mathbb{Z}_{22} \rightarrow \mathbb{Z}_{23}^{\otimes}$ given by $g(x) = 5^{x\otimes} = 5^x \bmod 23$.



Find the following:

$$\log_5^{\otimes}(1) = \underline{\hspace{1cm}}$$

$$\log_5^{\otimes}(5) = \underline{\hspace{1cm}}$$

$$\log_5^{\otimes}(9) = \underline{\hspace{1cm}}$$

$$\log_5^{\otimes}(10) = \underline{\hspace{1cm}}$$

$$\log_5^{\otimes}(14) = \underline{\hspace{1cm}}$$

$$\log_5^{\otimes}(17) = \underline{\hspace{1cm}}$$

$$\log_5^{\otimes}(20) = \underline{\hspace{1cm}}$$

Problem 15.4 (3) (1 point)

In $(\mathbb{Z}_{13}^{\otimes}, \otimes)$ where $a \otimes b = (a \cdot b) \bmod 13$ compute:

$$7^{0\otimes} = \underline{\hspace{1cm}}$$

$$7^{1\otimes} = \underline{\hspace{1cm}}$$

$$7^{2\otimes} = \underline{\hspace{1cm}}$$

$$7^{3\otimes} = \underline{\hspace{1cm}}$$

$$7^{4\otimes} = \underline{\hspace{1cm}}$$

$$7^{5\otimes} = \underline{\hspace{1cm}}$$

$$7^{6\otimes} = \underline{\hspace{1cm}}$$

$$7^{7\otimes} = \underline{\hspace{1cm}}$$

$$7^{8\otimes} = \underline{\hspace{1cm}}$$

$$7^{9\otimes} = \underline{\hspace{1cm}}$$

$$7^{10\otimes} = \underline{\hspace{1cm}}$$

$$7^{11\otimes} = \underline{\hspace{1cm}}$$

Now use the information above to find the following:

$$\log_7^{\otimes} 1 = \underline{\hspace{1cm}}$$

$$\log_7^{\otimes} 2 = \underline{\hspace{1cm}}$$

$$\log_7^{\otimes} 3 = \underline{\hspace{1cm}}$$

$$\log_7^{\otimes} 4 = \underline{\hspace{1cm}}$$

$$\log_7^{\otimes} 5 = \underline{\hspace{1cm}}$$

$$\log_7^{\otimes} 6 = \underline{\hspace{1cm}}$$

$$\log_7^{\otimes} 7 = \underline{\hspace{1cm}}$$

$$\log_7^{\otimes} 8 = \underline{\hspace{1cm}}$$

$$\log_7^{\otimes} 9 = \underline{\hspace{1cm}}$$

$$\log_7^{\otimes} 10 = \underline{\hspace{1cm}}$$

$$\log_7^{\otimes} 11 = \text{---}$$

$$\log_7^{\otimes} 12 = \text{---}$$

Problem 15.4 (4) (1 point)

In $(\mathbb{Z}_7^{\otimes}, \otimes)$ where $a \otimes b = (a \cdot b) \bmod 7$ compute:

$$2^{0\otimes} = \text{---}$$

$$2^{1\otimes} = \text{---}$$

$$2^{2\otimes} = \text{---}$$

$$2^{3\otimes} = \text{---}$$

$$2^{4\otimes} = \text{---}$$

$$2^{5\otimes} = \text{---}$$

$$2^{6\otimes} = \text{---}$$

Now use the information above to find the following:

$$\log_2^{\otimes}(1) = \text{---}$$

Problem 15.4 (5) (1 point)

Let $\otimes : \mathbb{Z}_{11}^{\otimes} \times \mathbb{Z}_{11}^{\otimes} \rightarrow \mathbb{Z}_{11}^{\otimes}$ be given by $a \otimes b = (a \cdot b) \bmod 11$.

In $(\mathbb{Z}_{11}^{\otimes}, \otimes)$ find the discrete logarithm of 7 to the base 7.

$$\log_7^{\otimes}(7) = \text{---}$$

Problem 15.4 (6) (1 point)

Let $\otimes : \mathbb{Z}_{17}^{\otimes} \times \mathbb{Z}_{17}^{\otimes} \rightarrow \mathbb{Z}_{17}^{\otimes}$ be given by $a \otimes b = (a \cdot b) \bmod 17$.

Find smallest non-negative integer n such that $14^{n\otimes} = 3$.

$$n = \text{---}$$

Problem 15.4 (7) (1 point)

Let $\otimes : \mathbb{Z}_5^\otimes \times \mathbb{Z}_5^\otimes \rightarrow \mathbb{Z}_5^\otimes$ be given by $a \otimes b = (a \cdot b) \bmod 5$.

In $(\mathbb{Z}_5^\otimes, \otimes)$ find the discrete logarithm of 4 to the base 4.

$\log_4^\otimes(4) = \underline{\hspace{2cm}}$

Solutions

Problem 15.4 (1) *Correct Answers:*

- 1
- 4
- 3
- 12
- 9
- 10
- 1
- 4
- 3
- 12
- 9
- 10
- 1
- 0

Problem 15.4 (2) *Correct Answers:*

Hint: The graph of the function $g : \mathbb{Z}_{23-1} \rightarrow \mathbb{Z}_{23}^{\otimes}$ given by $g(x) = 5^{x^{\otimes}} = 5^x \bmod 23$ is

$$\{(x, 5^x \bmod 23) \mid x \in \mathbb{Z}_{22}\} \subseteq \mathbb{Z}_{22} \rightarrow \mathbb{Z}_{23}^{\otimes}$$

In the plot the elements of the graph are represented by black pixels.

The discrete logarithm $\log_5^{\otimes}(y)$ to base 5 is the inverse of the exponential $5^{x^{\otimes}}$. That is, when $5^{x^{\otimes}} = y$ then $x = \log_5^{\otimes}(y)$.

Correct Answers:

- 0
- 1
- 10
- 3
- 21
- 7
- 5

Problem 15.4 (3) *Correct Answers:*

- 1
- 7
- 10
- 5
- 9
- 11
- 12
- 6
- 3
- 8

- 4
- 2
- 0
- 11
- 8
- 10
- 3
- 7
- 1
- 9
- 4
- 2
- 5
- 6

Problem 15.4 (4) *Correct Answers:*

- 1
- 2
- 4
- 1
- 2
- 4
- 1
- 0

Problem 15.4 (5) *Correct Answers:*

Hint: $\log_7^\otimes(7)$ is the smallest non-negative integer n such that $7^{n\otimes} = 7$.

Correct Answers:

- 1

Problem 15.4 (6) *Correct Answers:*

Hint: The smallest non-negative integer n such that $14^{n\otimes} = 3$ is the discrete logarithm of 3 to the base 14 in $(\mathbb{Z}_{17}^\otimes, \otimes)$ denoted by $\log_{14}^\otimes(3)$.

Correct Answers:

- 9

Problem 15.4 (7) *Correct Answers:*

Hint: $\log_4^\otimes(4)$ is the smallest non-negative integer n such that $4^{n\otimes} = 4$.

Correct Answers:

- 1

Chapter 16

Public Key Cryptography

1. Introduction Public Key
2. Diffie Hellman
3. ElGamal Crypto System

16.1 Introduction Public Key

Problem 16.1 (1) (1 point)

Complete the following.

A trapdoor function is an _____ function such that:

[select: | **easy** | **hard** | **impossible** | **invertible**]

(a) The function is _____ to evaluate.

[select: | **easy** | **hard** | **impossible** | **invertible**]

(b) The inverse of the function is _____ to evaluate when not in possession of some additional information.

[select: | **easy** | **hard** | **impossible** | **invertible**]

(c) The inverse of the function is _____ to evaluate when in possession of some additional information.

[select: | **easy** | **hard** | **impossible** | **invertible**]

Problem 16.1 (2) (1 point)

Computing $663634 - 939021$ ^(A) _____ computing $-275387 + 939021$. So subtraction is ^(B) _____ for a trapdoor function.

(A): [select: | **is much easier than** | **is much harder than** | **is about as difficult as**]

(B): [select: | **a candidate** | **not a candidate**]

Let $\otimes : \mathbb{Z}_{19759} \times \mathbb{Z}_{19759}^{\otimes} \rightarrow \mathbb{Z}_{19759}^{\otimes}$ be given by $a \otimes b = (a \cdot b) \bmod 19759$.

Computing $3^{14 \otimes}$ ^(A) _____ computing $\log_3^{\otimes} 1291$. So exponentiation modulo 19759 with the inverse discrete

logarithm is (B) for a trapdoor function.

(A): [select: | **is much easier than** | **is much harder than** | **is about as difficult as**]

(B): [select: | **a candidate** | **not a candidate**]

Problem 16.1 (3) (1 point)

Complete the following.

In public key cryptography:

Bob generates a key pair consisting of a (A) which he does not share with anyone and a(n) (B).

(A): [select: | **car key** | **house key** | **private key** | **public key**]

(B): [select: | **car key** | **house key** | **private key** | **public key**]

Bob publishes his (C) in a public key directory.

(C): [select: | **car key** | **house key** | **private key** | **public key**]

When Alice wants to send an encrypted message to Bob she looks up Bob's (D) in the public key directory. She uses Bob's (E) to encrypt a(n) (F) and sends the (G) to Bob.

(D): [select: | **car key** | **house key** | **private key** | **public key**]

(E): [select: | **car key** | **house key** | **private key** | **public key**]

(F): [select: | **encrypted message** | **message in plain text** | **mathematics book**]

(G): [select: | **encrypted message** | **message in plain text** | **mathematics book**]

When he receives a(n) (H) Bob decrypts it using his (I) to obtain the (J).

(H): [select: | **encrypted message** | **message in plain text** | **mathematics book**]

(I): [select: | **car key** | **house key** | **private key** | **public key**]

(J): [select: | **encrypted message** | **message in plain text** | **mathematics book**]

Solutions

Problem 16.1 (1) *Correct Answers:*

- invertible
- easy
- hard
- easy

Problem 16.1 (2) *Correct Answers:*

First Part:

Hint: If you can perform both computations by hand and/or a calculator with moderate effort, then the difficulty of both is most likely the same.

If one of the computations takes a lot of trying around and you still cannot perform it, then that computation is harder and the other easier.

Second Part:

Hint: If you can perform both computations by hand and/or a calculator with moderate effort, then the difficulty of both is most likely the same.

If one of the computations takes a lot of trying around and you still cannot perform it, then that computation is harder and the other easier.

Correct Answers:

- is about as difficult as
- not a candidate
- is much easier than
- a candidate

Problem 16.1 (3) *Correct Answers:*

- private key
- public key
- public key
- public key
- public key
- message in plain text
- encrypted message
- encrypted message
- private key
- message in plain text

16.2 Diffie Hellman

Problem 16.2 (1) (1 point)

In the Diffie Hellman Key Exchange:

Alice and Bob agree on a prime number p and a generator g for the group $(\{1, 2, 3, \dots, p-1\}, *)$ where $a * b = (a \cdot b) \bmod p$.

In the dropdown menus we write g^c for $g^{c*} = (g^c) \bmod p$.

Bob chooses an element b in $\{1, 2, 3, \dots, p-1\}$ and computes $B :=$ _____.

[select: | $g * a$ | $g * b$ | g^a | g^b | g^p | A^b | B^a]

Alice chooses an element a in $\{1, 2, 3, \dots, p-1\}$ and computes $A :=$ _____.

[select: | $g * a$ | $g * b$ | g^a | g^b | g^p | A^b | B^a]

Bob sends _____ to Alice. [select: | a | b | g | p | A | B]

Alice sends _____ to Bob. [select: | a | b | g | p | A | B]

Alice receives _____ from Bob. [select: | a | b | g | p | A | B]

Bob receives _____ from Alice. [select: | a | b | g | p | A | B]

Bob computes the shared secret _____.

[select: | $g * a$ | $g * b$ | g^a | g^b | g^p | A^b | B^a]

Alice computes the shared secret _____.

[select: | $g * a$ | $g * b$ | g^a | g^b | g^p | A^b | B^a]

The shared secret is equal to:
(Check all that apply)

- A. $(g^{a*})^{b*}$
- B. $(g^{b*})^{A*}$
- C. B^{a*}
- D. $a * b$
- E. A^{g*}
- F. $g * (a * b)$
- G. $g^{(ab)*}$
- H. $(g^{b*})^{a*}$
- I. $A * B$
- J. B^{p*}
- K. A^{B*}
- L. $(g^{b*}) * a$
- M. A^{b*}

Problem 16.2 (2) (1 point)

Alice and Bob use the Diffie Hellman key exchange to generate a shared secret.

Alice and Bob

For their Diffie Hellman key exchange Alice and Bob agree to work in the group of $(\mathbb{Z}_{1759}^{\otimes}, \otimes)$ where $a \otimes b = (a \cdot b) \bmod 1759$. They also agree on the generator $g = 6$.

Alice

Alice chooses her secret $a = 3$ and sends $A = \underline{\hspace{1cm}}$ to Bob.

Bob

Bob chooses his secret $b = 2$ and sends $B = \underline{\hspace{1cm}}$ to Alice.

Alice

Alice receives $B = \underline{\hspace{1cm}}$ from Bob computes the shared secret $\underline{\hspace{1cm}}$.

Bob

Bob receives $A = \underline{\hspace{1cm}}$ from Alice computes the shared secret $\underline{\hspace{1cm}}$.

Problem 16.2 (3) (1 point)

For a Diffie-Hellman key exchange Alice and Bob use the group $(\mathbb{Z}_{11}^{\otimes}, \otimes)$ and the generator $g = 2$.

Bob chooses $b = 8$ as his secret.

What does Bob send to Alice ?

$B = \underline{\hspace{1cm}}$.

Problem 16.2 (4) (1 point)

For a Diffie-Hellman key exchange Alice and Bob use the group $(\mathbb{Z}_{17}^{\otimes}, \otimes)$ and the generator $g = 2$.

Alice sends $A = 8$ to Bob and Bob chooses $b = 7$ as his secret.

The shared secret is $s = \underline{\hspace{1cm}}$.

Problem 16.2 (5) (1 point)

Alice and Bob use the Diffie Hellman key exchange to generate a shared secret.

Alice and Bob: The Group

For their Diffie Hellman key exchange Alice and Bob agree to work in the group of $(\mathbb{Z}_{19}^{\otimes}, \otimes)$ where $a \otimes b = (a \cdot b) \bmod 19$. They also agree on the generator $g = 2$.

Alice: Secret

Alice chooses her secret $a = 5$ and sends $A = g^{a \otimes} = (g^a) \bmod 19 = \underline{\hspace{1cm}}$ to Bob.

Bob: Secret

Bob chooses his secret $b = 4$ and sends $B = g^{b \otimes} = (g^b) \bmod 19 = \underline{\hspace{1cm}}$ to Alice.

Alice: Shared Secret

Alice receives $B = \underline{\hspace{1cm}}$ from Bob, and she computes the shared secret $B^{a \otimes} = (B^a) \bmod 19 = \underline{\hspace{1cm}}$.

Bob: Shared Secret

Bob receives $A = \underline{\hspace{1cm}}$ from Alice, and he computes the shared secret $A^{b \otimes} = (A^b) \bmod 19 = \underline{\hspace{1cm}}$.

Alice and Bob: Shared Secret

Now Alice and Bob share the secret ____.

Problem 16.2 (6) (1 point)

Alice and Bob use the Diffie Hellman key exchange to generate a shared secret.

Alice and Bob: The Group

Alice and Bob agree to work in the subgroup of $(\mathbb{Z}_{1747}^{\otimes}, \otimes)$ where $a \otimes b = (a \cdot b) \bmod 1747$ generated by $g = 2 \in \mathbb{Z}_{1747}^{\otimes}$ for their key exchange.

Alice: Secret

Alice chooses her secret $a = 4$ and sends $A = (g^a) \bmod p = \underline{\hspace{1cm}}$ to Bob.

Bob: Secret

Bob chooses his secret $b = 5$ and sends $B = (g^b) \bmod p = \underline{\hspace{1cm}}$ to Alice.

Alice: Shared Secret

Alice receives $B = \underline{\hspace{1cm}}$ from Bob computes the shared secret $(B^a) \bmod p = \underline{\hspace{1cm}}$.

Bob: Shared Secret

Bob receives $A = \underline{\hspace{1cm}}$ from Alice computes the shared secret $(A^b) \bmod p = \underline{\hspace{1cm}}$.

Alice and Bob: Shared Secret

Now Alice and Bob share the secret ____.

Problem 16.2 (7) (1 point)

In the following we demonstrate the use of the Diffie-Hellman key exchange together with a symmetric cipher. For demonstration purposes only the symmetric cipher is a Caesar cipher. In the real world the numbers in the Diffie-Hellman key exchange are much larger and the symmetric cipher is a cipher that is more secure than the Caesar cipher; for example the Advanced Encryption Standard – AES.

First Alice and Bob use the Diffie Hellman key exchange to generate a shared secret.

Alice and Bob: The Group

For their Diffie Hellman key exchange Alice and Bob agree to work in the group of $(\mathbb{Z}_{13}^{\otimes}, \otimes)$ where $a \otimes b = (a \cdot b) \bmod 13$. They also agree on the generator $g = 2$.

Alice: Secret

Alice chooses her secret $a = 7$ and sends $A = g^{a \otimes} = (g^a) \bmod 13 = \underline{\hspace{1cm}}$ to Bob.

Bob: Secret

Bob chooses his secret $b = 4$ and sends $B = g^{b \otimes} = (g^b) \bmod 13 = \underline{\hspace{1cm}}$ to Alice.

Alice: Shared Secret

Alice receives $B = \underline{\hspace{1cm}}$ from Bob, and she computes the shared secret $B^{a \otimes} = (B^a) \bmod 13 = \underline{\hspace{1cm}}$.

Bob: Shared Secret

Bob receives $A = \underline{\hspace{1cm}}$ from Alice, and he computes the shared secret $A^{b \otimes} = (A^b) \bmod 13 = \underline{\hspace{1cm}}$.

Now Alice and Bob use their shared secret s as the key in a Caesar cipher, that is, the number of letters by which they shift the characters is s .

Alice: Encryption

Alice wants to send the secret message `smile` to Bob. She encrypts `smile` with the Caesar cipher shifting by $s = \underline{\hspace{1cm}}$ characters. The encrypted message is `_____`. Alice sends the encrypted message to Bob.

Bob: Decryption

Bob receives the encrypted message `_____` from Alice. He decrypts it with the Caesar cipher shifting

by $s = ______$ characters and obtains the plain text $______$.

Solutions

Problem 16.2 (1) *Correct Answers:*

- g^b
 - g^a
 - B
 - A
 - B
 - A
 - A^b
 - B^a
 - ACGHM
-

Problem 16.2 (2) *Correct Answers:*

- 216
 - 36
 - 36
 - 922
 - 216
 - 922
-

Problem 16.2 (3) *Correct Answers:*

- 3
-

Problem 16.2 (4) *Correct Answers:*

- 15
-

Problem 16.2 (5) *Correct Answers:*

- 13
- 16
- 16
- 4
- 13
- 4
- 4

Problem 16.2 (6) *Correct Answers:*

- 16
- 32
- 32
- 376
- 16
- 376
- 376

Problem 16.2 (7) *Correct Answers:*

- 11
- 3
- 3
- 3
- 11
- 3
- 3
- pjfib
- pjfib
- 3
- smile

16.3 ElGamal Crypto System

Problem 16.3 (1) (1 point)

When using the ElGamal cryptosystem Bob and Alice do the following.

Bob: Key generation

To generate his public key Bob chooses a prime number p and a generator g in the group $(\{1, 2, 3, \dots, p-1\}, *)$ where $a * b = (a \cdot b) \bmod p$.

In the dropdown menus we write g^c for g^{c*} .

Bob chooses an element b in $\{1, 2, 3, \dots, p-1\}$ and computes $B :=$ _____.

[select: | g^a | g^b | g^a | g^b | g^p | A^b | B^a | m^s | X^t]

Bob publishes his public key _____. [select: | (a, X) | (A, X) | (B, X) | (g, b, B) | (p, g, b) | (p, g, B) | (p, b, B)]

Alice: Encryption

Alice wants to send the secret message m to Bob.

Alice obtains Bob's public key _____ from the public key directory.

[select: | (a, X) | (A, X) | (B, X) | (g, b, B) | (p, g, b) | (p, g, B) | (p, b, B)]

Alice chooses a in $\{1, 2, 3, \dots, p-1\}$ and computes $A :=$ _____.

[select: | g^a | g^b | g^a | g^b | g^p | A^b | B^a | m^s | X^t]

Alice computes the shared secret $s :=$ _____.

[select: | g^a | g^b | g^a | g^b | g^p | A^b | B^a | m^s | X^t]

To encrypt m in $\{1, 2, 3, \dots, p-1\}$ Alice computes $X :=$ _____.

[select: | g^a | g^b | g^a | g^b | g^p | A^b | B^a | m^s | X^t]

Alice sends _____ to Bob.

[select: | (a, X) | (A, X) | (A, m) | (B, X) | (s, m) | (s, X)]

Bob: Decryption

Bob receives _____ from Alice.

[select: | (a,X) | (A,X) | (A,m) | (B,X) | (s,m) | (s,X)]

Bob computes the shared secret _____.

[select: | g^*a | g^*b | g^a | g^b | g^p | A^b | B^a | $m*s$ | $X*t$]

Bob computes the inverse t of s in the group $(\{1, 2, 3, \dots, p-1\}, *)$.

Bob obtains the message m by computing _____.

[select: | g^*a | g^*b | g^a | g^b | g^p | A^b | B^a | $m*s$ | $X*t$]

Problem 16.3 (2) (1 point)

Alice and Bob use the ElGamal cryptosystem for their secure communication.

Bob: Key Generation

Bob chooses the prime $p = 7$. So he will work in the group $(\mathbb{Z}_7^\otimes, \otimes)$ where $a \otimes b = (a \cdot b) \bmod 7$. He chooses $g = 3 \in \mathbb{Z}_7^\otimes$.

Bob chooses his secret key $b = 3$ and computes $B = (g^b) \bmod p = ______$.

Bob publishes p , g , and B in the public key directory.

Directory of Public Keys

Aaron: $p = 31$, $g = 8$, $B = 2$

Alice: $p = 23$, $g = 2$, $B = 6$

Bob: $p = ______$, $g = ______$, $B = ______$

Sebastian: $p = 19$, $g = 13$, $B = 2$

Victoria: $p = 31$, $g = 8$, $B = 16$

Alice: Encryption

Alice wants to send the message $m = 3$ to Bob.

Bob: Decryption

Bob receives A and X from Alice.

Bob computes the shared secret $s = (A^b) \bmod p = \underline{\hspace{1cm}}$.

Bob finds the inverse $s^{-1} = \underline{\hspace{1cm}}$ of s in the group $(\mathbb{Z}_7^\otimes, \otimes)$.

Bob decrypts the message by computing $M = (X \cdot s^{-1}) \bmod p = \underline{\hspace{1cm}}$.

Hint: In $(\mathbb{Z}_7^\otimes, \otimes)$ we have

$$1^{-1\otimes} = 1, 2^{-1\otimes} = 4, 3^{-1\otimes} = 5, 4^{-1\otimes} = 2, 5^{-1\otimes} = 3, 6^{-1\otimes} = 6$$

Problem 16.3 (3) (1 point)

Alice and Bob use the ElGamal cryptosystem for their secure communication.

Bob: Key Generation

Bob chooses the prime $p = 7$ and the generator $g = 3 \in \mathbb{Z}_7^\otimes$.

Bob chooses his secret key $b = 2$ and computes $B = (g^b) \bmod 7 = \underline{\hspace{1cm}}$.

Bob publishes p , g , and B in the public key directory.

Directory of Public Keys

Bob: $p = \underline{\hspace{1cm}}, g = \underline{\hspace{1cm}}, B = \underline{\hspace{1cm}}$

Nathan: $p = 31, g = 8, B = 16$

Thom: $p = 47, g = 1, B = 1$

Bob: Decryption

Bob receives $A = 6$ and $X = 2$ from Alice.

Bob computes the shared secret $s = (A^b) \bmod 7 = \underline{\hspace{1cm}}$.

Bob finds the inverse $s^{-1} = \underline{\hspace{1cm}}$ of s in the group $(\mathbb{Z}_7^\otimes, \otimes)$.

Bob decrypts the message by computing $M = (X \cdot s^{-1}) \bmod 7 = \underline{\hspace{1cm}}$.

Hint: In $(\mathbb{Z}_7^\otimes, \otimes)$ we have

$$1^{-1\otimes} = 1, 2^{-1\otimes} = 4, 3^{-1\otimes} = 5, 4^{-1\otimes} = 2, 5^{-1\otimes} = 3, 6^{-1\otimes} = 6,$$

Problem 16.3 (4) (1 point)

Alice and Bob use the ElGamal cryptosystem for their secure communication.

Bob: Key Generation

Bob chooses the prime $p = 19753$ and the generator $g = 5 \in \mathbb{Z}_{19753}^\otimes$.

Bob chooses his secret key $b = 6 \in \mathbb{Z}_{19753}^\otimes$ and computes $B = (g^b) \bmod 19753 = \underline{\hspace{1cm}}$.

Bob publishes p , g , and B in the public key directory.

Directory of Public Keys Aaron: $p = 19793, g = 243, B = 393$

Beth: $p = 19801, g = 18949, B = 2072$

Bob: $p = \underline{\hspace{1cm}}, g = \underline{\hspace{1cm}}, B = \underline{\hspace{1cm}}$

Sebastian: $p = 19913, g = 243, B = 1205$

Victoria: $p = 19751, g = 13752, B = 1679$

Bob: Decryption

Bob receives $A = 125$ and $X = 12075$ from Alice.

Bob computes the shared secret $s = (A^b) \bmod 19753 = \underline{\hspace{1cm}}$.

Bob computes the inverse $s^{-1} = 11561$ of s in the group $(\mathbb{Z}_{19753}^\otimes, \otimes)$.

Bob decrypts the message by computing $M = (X \cdot s^{-1}) \bmod 19753 = \underline{\hspace{1cm}}$.

Bob finds the expanded base 27 form of M , namely $M = \underline{\hspace{1cm}} \cdot 27^2 + \underline{\hspace{1cm}} \cdot 27 + \underline{\hspace{1cm}}$.

Decoding these numbers with C^{-1} yields the message $\underline{\hspace{1cm}}$.

Problem 16.3 (5) (1 point)

Alice and Bob use the ElGamal cryptosystem for their secure communication.

When generating his key pair Bob chooses $p = 13$ and $g = 2$.

That is, he decides to work in the subgroup $\langle 2 \rangle$ of $(\mathbb{Z}_{13}^\otimes, \otimes)$ where $a \otimes b = (a \cdot b) \bmod 13$.

Bob chooses his secret key $b = 2$ and computes $B = g^{b \otimes} = ___$.

The values that Bob publishes in the public key directory are:

$p = ___, g = ___,$ and $B = ___$

Problem 16.3 (6) (1 point)

Alice and Bob use the ElGamal cryptosystem for their secure communication. Alice sends an encrypted message to Bob.

Directory of Public Keys

Bob: $p = 19759, g = 3, B = 27$

Nathan: $p = 19867, g = 128, B = 14383$

Thom: $p = 19913, g = 243, B = 11547$

Alice: Encryption

Alice wants to send the message 'eve' to Bob.

Alice gets Bob's public key from the directory: $p = ___, g = ___, B = ___$

She applies the encoding function $C : \{-, a, b, c, \dots, z\} \rightarrow \{0, 1, 2, 3, \dots, 26\}$ with $C(-) = 0, C(a) = 1, \dots, C(z) = 26$ to the characters in message. She obtains $C(e) = ___, C(v) = ___,$ and $C(e) = ___$.

She encodes this into one number by computing $m = C(e) \cdot 27^2 + C(v) \cdot 27 + C(e) = ___$.

Alice chooses her secret $a = 3$.

Alice computes the shared secret $s = (B^a) \bmod p = ___$.

She computes $A = (g^a) \bmod p = ___$.

Alice encrypts the message by computing $X = (m \cdot s) \bmod p = ___$.

Alice sends A and X to Bob.

Problem 16.3 (7) (1 point)

Alice and Bob use the El Gamal crypto system for their secure communication.

Bob's public key is $p = 13, g = 2, B = 12$

Alice sends $A = 2$ and $X = 4$ to Bob.

Bob decrypts this message using his private key $b = 6$ and obtains $m = \underline{\hspace{1cm}}$.

Hint: In the group $\mathbb{Z}_{13}^{\otimes}$, $\otimes$ where $a \otimes b = (a \cdot b) \bmod 13$ we have

$1^{-1 \otimes} = 1, 2^{-1 \otimes} = 7, 3^{-1 \otimes} = 9, 4^{-1 \otimes} = 10, 5^{-1 \otimes} = 8, 6^{-1 \otimes} = 11, 7^{-1 \otimes} = 2, 8^{-1 \otimes} = 5, 9^{-1 \otimes} = 3, 10^{-1 \otimes} = 4,$
 $11^{-1 \otimes} = 6, 12^{-1 \otimes} = 12,$

Problem 16.3 (8) (1 point)

Alice and Bob use the ElGamal crypto system for their secure communication.

From the key directory Alice obtains Bob's public key is $p = 5, g = 2, B = 3$.

Alice chooses her secret $a = 2$ and computes the shared secret $s = \underline{\hspace{1cm}}$.

Alice encrypts the message $m = 2$ and sends $A = \underline{\hspace{1cm}}$ and $X = \underline{\hspace{1cm}}$ to Bob.

Problem 16.3 (9) (1 point)

Alice and Bob use the El Gamal crypto system for their secure communication.

Bob: Key Generation

Bob chooses the prime $p = 19927$ and the generator $g = 6 \in \mathbb{Z}_{19927}^{\otimes}$.

Bob chooses his secret key $b = 2$ and computes $B = (g^b) \bmod p = \underline{\hspace{1cm}}$.

Bob publishes $p, g,$ and B in the public key directory.

Directory of Public Keys Aaron: $p = 19819, g = 243, B = 1776$

Beth: $p = 19861, g = 3530, B = 5462$

Bob: $p = \underline{\hspace{1cm}}, g = \underline{\hspace{1cm}}, B = \underline{\hspace{1cm}}$

Sebastian: $p = 19891, g = 32, B = 7993$

Victoria: $p = 19919, g = 6864, B = 5492$

Bob: Decryption

Bob receives A and X from Alice.

Bob computes the shared secret $s = (A^b) \bmod p = \underline{\hspace{1cm}}$.

Bob computes the inverse $s^{-1} = 12439$ of s in the group $(\mathbb{Z}_{19927}^{\otimes}, \otimes)$.

Bob decrypts the message by computing $M = (X \cdot s^{-1}) \bmod p = \underline{\hspace{1cm}}$.

Bob finds the expanded base 27 form of M , namely $M = \underline{\hspace{1cm}} \cdot 27^2 + \underline{\hspace{1cm}} \cdot 27 + \underline{\hspace{1cm}}$.

Decoding these numbers with C^{-1} yields the message $\underline{\hspace{1cm}}$.

Solutions

Problem 16.3 (1) *Correct Answers:*

- g^b
- (p, g, B)
- (p, g, B)
- g^a
- B^a
- m^s
- (A, X)
- (A, X)
- A^b
- X^t

Problem 16.3 (2) *Correct Answers:*

- 6
- 7
- 3
- 6
- 7
- 3
- 6
- 1
- 2
- 3
- 1
- 1
- 3

Problem 16.3 (3) *Correct Answers:*

- 2
- 7
- 3
- 2
- 1
- 1
- 2

Problem 16.3 (4) Correct Answers:

- 15625
- 19753
- 5
- 15625
- 19196
- 4624
- 6
- 9
- 7
- FIG

Problem 16.3 (5) Correct Answers:

- 4
- 13
- 2
- 4

Problem 16.3 (6) Correct Answers:

- 19759
- 3
- 27
- 5
- 22
- 5
- 4244
- 19683
- 27
- 13359

Problem 16.3 (7) Correct Answers:

Hint: The shared secret is $s = A^{b \otimes}$.

The decrypted message is $m = X \otimes s^{-1 \otimes}$ where $s^{-1 \otimes}$ is the inverse of s with respect to $\otimes$.

- 9

Problem 16.3 (8) Correct Answers:

- 4
- 4
- 3

Problem 16.3 (9) *Correct Answers:*

- 36
- 19927
- 6
- 36
- 19927
- 6
- 36
- 1
- 12
- 5
- 1058
- 1296
- 36
- 16132
- 1296
- 1058
- 1
- 12
- 5
- ale