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

February 19, 2024

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

Contents

Chapter 1

Foundations

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

1.1 Integers

Problem 1.1 (1) Fill in the blank.

The numbers $1, 2, 3, 4, \ldots$ 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 $\ldots, -4, -3, -2, -1$ 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:

$4-6=$ ____

$10-2=$ ____

$2-17=$ ____

Problem 1.1 (6) **(1 point)**

Multiply the following integers.

a. $(-9)\cdot(-1)=$ ____

b. $(-5)\cdot 2=$ ____

c. $6 \cdot (-7) =$ ____

d. $(-6) \cdot 0 =$ ____

Problem 1.1 (7) **(1 point)**

Add the following:

$-8+(-2) =$ ____

$-6+(-5) =$ ____

$-1+(-8) =$ ____

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

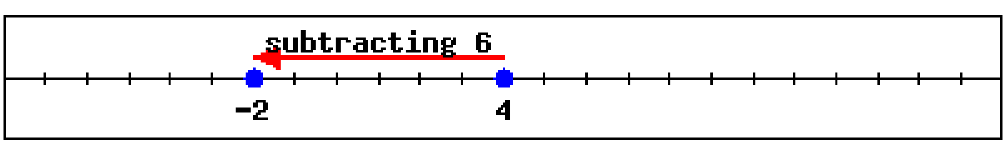
Problem 1.1 (5) *Correct Answers:*
Solution:

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

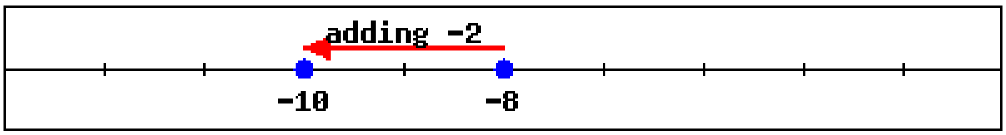
Problem 1.1 (7) *Correct Answers:*
Solution:

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 than 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 than 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: $a = 6$, $b = 8$, $c =$___.

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: $a = 4$, $b =$___

(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: $a = 4$, $b = 5$, $c =$___

(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: $a =$___, $b = 5$, $c = 4$.

Problem 1.3 (7) (1 point)

The additive inverse of 14876 is ________.

Problem 1.3 (8) (1 point)

Anwer 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 $a\cdot b=b\cdot a$.

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

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

A. Distributive property

B. Commutative property of multiplication

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: $a =$___

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 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:

$0^6 =$ ___

$1^6 =$ ___

$2^6 =$ ___

$3^6 =$ ___

$4^6 =$ ___

$5^6 =$ ___

Problem 1.4 (2) (1 point)

Compute:

$4^0 =$ ___

$4^1 =$ ___

$4^2 =$ ___

$4^3 =$ ___

$4^4 =$ ___

$4^5 =$ ___

$4^6 =$ ___

$4^7 =$ ___

$4^8 =$ ___

$4^9 =$ ___

$4^{10} =$ ___

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‘ˆc) you enter the answer in the form x ˆ c, where c is an integer.

$x^7 \cdot x^{18}$=______

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 ˆ x, where x is an integer.

$3^6 \cdot 3^2$=______

Problem 1.4 (9) (1 point)

Use the properties of exponents to simplify the following.

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

$(6^6)^6$=______

Problem 1.4 (10) (1 point)

Use the properties of exponents to simplify the following

$y^{18} \cdot y^{20} =$ ______

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

Problem 1.4 (11) (1 point)

Use the properties of exponents to simplify the following

$$\left(y^4\right)^{11}$$

______

Example: Enter y^4 as yˆ4.

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:

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

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

$$\left(6^6\right)^6 = 6^{6\cdot 6}$$
$$= 6^{36}$$

Correct Answers:

- 6^{36}

Problem 1.4 (10) *Correct Answers:*

Solution:

We *add* the exponents as follows

$$y^{18} \cdot y^{20} = y^{18+20}$$
$$= y^{38}$$

Correct Answers:

- y^{38}

Problem 1.4 (11) *Correct Answers:*

Solution:

We *multiply* the exponents as follows

$$\left(y^4\right)^{11} = y^{4\cdot 11}$$
$$= y^{44}$$

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** $c \cdot h$

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 $n =$ ___.

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

(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 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 ende. 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 $b :=$ ___ an exponent $n :=$ ___.

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

let i:=i+1=___ and **let** $c := c \cdot 3 =$ ___.

let i:=i+1=___ and **let** $c := c \cdot 3 =$ ___.

let i:=i+1=___ and **let** $c := c \cdot 3 =$ ___.

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

Output: $c =$ ___

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 $n = 0$? ___
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 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

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 div 609018 = ____.

228628410848 mod 609018 = ____.

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 div 649166 = ____.

252125356168 mod 649166 = ____.

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 div b and $r = a \bmod b$.

Input: $a =$ ___ and $b =$ ___.

let $q := 0$ and **let** $r := a =$ ___.

let $q := q + 1 =$ ___ and **let** $r := r - 10 =$ ___.

let $q := q + 1 =$ ___ and **let** $r := r - 10 =$ ___.

let $q := q + 1 =$ ___ and **let** $r := r - 10 =$ ___.

let $q := q + 1 =$ ___ and **let** $r := r - 10 =$ ___.

Because $r < b$ the loop ends here.

Output: The quotient $q =$ ___ and the remainder $r =$ ___.

Problem 3.2 (2) (1 point)

Find the quotients and remainders:

10 div 4 = _____ and
10 mod 4 = _____

12 div 6 = _____ and
12 mod 6 = _____

17 div 8 = _____ and
17 mod 8 = _____

34 div 2 = _____ and
34 mod 2 = _____

32 div 2 = _____ and
32 mod 2 = _____

Problem 3.2 (3) (1 point)

Find the quotients and remainders:

6 div 7 = _____ and
6 mod 7 = _____

-32 div 8 = _____ and
-32 mod 8 = _____

19 div 5 = _____ and
19 mod 5 = _____

-27 div 3 = _____ and
-27 mod 3 = _____

Problem 3.2 (4) (1 point)

Division

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

Input: $a =$ ___ and $b =$ ___.

let $q := 0$ and **let** $r := a =$ ___.

let $q := q+1 =$ ___ and **let** $r := r-6 =$ ___.

let $q := q+1 =$ ___ and **let** $r := r-6 =$ ___.

let $q := q+1 =$ ___ and **let** $r := r-6 =$ ___.

let $q := q+1 =$ ___ and **let** $r := r-6 =$ ___.

let $q := q+1 =$ ___ and **let** $r := r-6 =$ ___.

let $q := q+1 =$ ___ and **let** $r := r-6 =$ ___.

let $q := q+1 =$ ___ and **let** $r := r-6 =$ ___.

let $q := q+1 =$ ___ and **let** $r := r-6 =$ ___.

let $q := q+1 =$ ___ and **let** $r := r-6 =$ ___.

let $q := q+1 =$ ___ and **let** $r := r-6 =$ ___.

let $q := q+1 =$ ___ and **let** $r := r-6 =$ ___.

Because $r < b$ the loop ends here.

Output: The quotient $q =$ ___ and the remainder $r =$ ___.

Problem 3.2 (5) (1 point)

Division

Let $a := -77$ and let $b := 14$. With the division algorithm find a div b and $r = a$ mod b.

Input: $a =$ ___ and $b =$ ___.

let $q := 0$ and **let** $r := a =$ ___.

let $q := q - 1 =$ ___ and **let** $r := r + 14 =$ ___.

let $q := q - 1 =$ ___ and **let** $r := r + 14 =$ ___.

let $q := q - 1 =$ ___ and **let** $r := r + 14 =$ ___.

let $q := q - 1 =$ ___ and **let** $r := r + 14 =$ ___.

let $q := q - 1 =$ ___ and **let** $r := r + 14 =$ ___.

let $q := q - 1 =$ ___ and **let** $r := r + 14 =$ ___.

Because $r > 0$ the loop ends here.

Output: The quotient $q =$ ___ and the remainder $r =$ ___.

Problem 3.2 (6) (1 point)

Division

Let $a := 92$ and let $b := 26$. With the division algorithm find a div b and $r = a$ mod b.

Input: $a =$ ___ and $b =$ ___.

let $q := 0$ and **let** $r := a =$ ___.

let $q := q + 1 =$ ___ and **let** $r := r - 26 =$ ___.

let $q := q + 1 =$ ___ and **let** $r := r - 26 =$ ___.

let $q := q + 1 =$ ___ and **let** $r := r - 26 =$ ___.

Because $r < b$ the loop ends here.

Output: The quotient $q =$ ___ and the remainder $r =$ ___.

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 $m := 2$? ___
What does the algorithm return when the input is $n := 4$ and $m := 2$? ___
What does the algorithm return when the input is $n := 6$ and $m := 2$? ___

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=___ and r=___

What does the algorithm return when the input is $n := 5$ and $m := 3$?
q=___ and r=___

What does the algorithm return when the input is $n := 13$ and $m := 5$?
q=___ and r=___

What does the algorithm return when the input is $n := 7$ and $m := 2$?
q=___ and r=___

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 $n := 5$? ___
What does the algorithm return when the input is $n := 7$? ___
What does the algorithm return when the input is $n := 15$? ___
What does the algorithm return when the input is $n := 33$? ___

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 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 div 50 = 9

and

a mod 50 = 27.

Then a=___

Problem 3.2 (13) (1 point)

Find the quotient and remainder:

-8 div 71 = ___

-8 mod 71 = ___

Problem 3.2 (14) (1 point)

Find the quotient and remainder:

70 div 24 = ___

70 mod 24 = ___

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 $d := 5349 \div 73 =$ ___.

The quotient q is the integer to the left of d on the number line. Thus $q =$ ___.

The remainder is $r := 5349 - (73 \cdot q) =$ ___.

So we have found that 5349 div 73 =___ and 5349 mod 73 =___.

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 $d := -6367 \div 2612 =$ ___.

The quotient q is the integer to the left of d on the number line. Thus $q =$ ___.

The remainder is $r := -6367 - (2612 \cdot q) =$ ___.

So we have found that -6367 div 2612 =___ and -6367 mod 2612 =___.

Problem 3.3 (3) (1 point)

Find the quotients and remainders:

4550 div 678 = _____ and
4550 mod 678 = _____

4733 div 560 = _____ and
4733 mod 560 = _____

2241 div 695 = _____ and
2241 mod 695 = _____

1567 div 697 = _____ and
1567 mod 697 = _____

2764 div 686 = _____ and
2764 mod 686 = _____

Problem 3.3 (4) **(1 point)**

Find the quotients and remainders:

59880 div 1997 = _____ and
59880 mod 1997 = _____

-98474 div 1070 = _____ and
-98474 mod 1070 = _____

54702 div 939 = _____ and
54702 mod 939 = _____

-83287 div 1288 = _____ and
-83287 mod 1288 = _____

Problem 3.3 (5) **(1 point)**

Find the quotient and remainder:

-30 div 78 = ___

-30 mod 78 = ___

Problem 3.3 (6) **(1 point)**

Find the quotient and remainder:

66 div 49 = ___

66 mod 49 = ___

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 mod 6 = ___

1 mod 6 = ___

2 mod 6 = ___

3 mod 6 = ___

4 mod 6 = ___

5 mod 6 = ___

6 mod 6 = ___

7 mod 6 = ___

8 mod 6 = ___

9 mod 6 = ___

10 mod 6 = ___

11 mod 6 = ___

12 mod 6 = ___

13 mod 6 = ___

Problem 3.4 (2) (1 point)

Compute 136 mod 182 = __________

Problem 3.4 (3) (1 point)

Compute:

0 mod 5 = ___ and 0 mod 6 = ___

1 mod 5 = ___ and 1 mod 6 = ___

2 mod 5 = ___ and 2 mod 6 = ___

3 mod 5 = ___ and 3 mod 6 = ___

4 mod 5 = ___ and 4 mod 6 = ___

5 mod 5 = ___ and 5 mod 6 = ___

6 mod 5 = ___ and 6 mod 6 = ___

7 mod 5 = ___ and 7 mod 6 = ___

8 mod 5 = ___ and 8 mod 6 = ___

9 mod 5 = ___ and 9 mod 6 = ___

10 mod 5 = ___ and 10 mod 6 = ___

11 mod 5 = ___ and 11 mod 6 = ___

Problem 3.4 (4) (1 point)

Compute:

0 mod 5 = ___ and 0 mod 3 = ___

1 mod 5 = ___ and 1 mod 3 = ___

2 mod 5 = ___ and 2 mod 3 = ___

3 mod 5 = ___ and 3 mod 3 = ___

4 mod 5 = ___ and 4 mod 3 = ___

5 mod 5 = ___ and 5 mod 3 = ___

6 mod 5 = ___ and 6 mod 3 = ___

7 mod 5 = ___ and 7 mod 3 = ___

8 mod 5 = ___ and 8 mod 3 = ___

9 mod 5 = ___ and 9 mod 3 = ___

10 mod 5 = ___ and 10 mod 3 = ___

11 mod 5 = ___ and 11 mod 3 = ___

12 mod 5 = ___ and 12 mod 3 = ___

13 mod 5 = ___ and 13 mod 3 = ___

14 mod 5 = ___ and 14 mod 3 = ___

Find the smallest non-negative integer b such that b mod $5 = 3$ and b mod $3 = 2$.
$b =$ ___

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 mod $33 = 6$ and b mod $33 = 10$.

Find:

$(a+a)$ mod 33 = ___

$(a+b)$ mod 33 = ___

$(a \cdot b)$ mod 33 = ___

$(a+9)$ mod 33 = ___

$(9 \cdot b)$ mod 33 = ___

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 mod $15 = 5$ and b mod $15 = 10$.

Find:

$(a+a)$ mod 15 = ___

$(a+b)$ mod 15 = ___

$(a \cdot b)$ mod 15 = ___

$(a+7)$ mod 15 = ___

$(7 \cdot b) \bmod 15 =$ ___

Problem 3.4 (7) (1 point)

Compute these remainders:

52 mod 19 = _____

4 mod 11 = _____

197 mod 9 = _____

12 mod 23 = _____

183 mod 33 = _____

76 mod 5 = _____

Problem 3.4 (8) (1 point)

We can write 2182460683 =_____ ·100+ ___

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

Because 83 mod 2 = ___ we have 2182460683 mod 2 = ___.

Because 83 mod 4 = ___ we have 2182460683 mod 4 = ___.

Because 83 mod 5 = ___ we have 2182460683 mod 5 = ___.

Because 83 mod 10 = ___ we have 2182460683 mod 10 = ___.

Because 83 mod 20 = ___ we have 2182460683 mod 20 = ___.

Because 83 mod 25 = ___ we have 2182460683 mod 25 = ___.

Because 83 mod 100 = ___ we have 2182460683 mod 100 = ___.

Problem 3.4 (9) (1 point)

What is the remainder of 23451638 divided by 5? ___

What is the remainder of 23451638 divided by 4? ___

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

Problem 3.4 (10) (1 point)

Compute:

23210494277064179722 mod 2 = ___

23210494277064179722 mod 4 = ___

23210494277064179722 mod 5 = ___

23210494277064179722 mod 10 = ___

23210494277064179722 mod 20 = ___

23210494277064179722 mod 25 = ___

23210494277064179722 mod 100 = ___

23210494277064179722 mod 1000 = ___

23210494277064179722 mod 10000 = ___

Problem 3.4 (11) (1 point)

Compute:

10249838952446438118 mod 10 = ____

10249838952446438118 mod 100 = ____

10249838952446438118 mod 1000 = ____

10249838952446438118 mod 10000 = ____

10249838952446438118 mod 100000 = ____

10249838952446438118 mod 1000000 = ____

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 mod 10 = 3 mod 10

Thus, because 2 and 5 divide 10, also

2182460683 mod 2 = 3 mod 2 and
2182460683 mod 5 = 3 mod 5

Similarly

2182460683 mod 100 = 83 mod 100

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

2182460683 mod 4 = 83 mod 4 and
2182460683 mod 20 = 83 mod 20 and
2182460683 mod 25 = 83 mod 25.

Correct Answers:

- 21824606
- 83
- 1
- 1
- 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

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

Similarly

$23210494277064179722 \bmod 100 = 22 \bmod 100$

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

$23210494277064179722 \bmod 4 = 22 \bmod 4$ and
$23210494277064179722 \bmod 20 = 22 \bmod 20$ 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

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

$z =$ ___

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

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

$z =$ ___

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

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

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

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

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

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

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 mod 14= ___ we have that 14 ________________ 61. [select: | **divides** | **does not divide**]

Because 21 mod 2= ___ we have that 2 ________________ 21. [select: | **divides** | **does not divide**]

Because 49 mod 5= ___ we have that 5 ________________ 49. [select: | **divides** | **does not divide**]

Because 81 mod 11= ___ we have that 11 ________________ 81. [select: | **divides** | **does not divide**]

Because 8 mod 20= ___ we have that 20 ________________ 8. [select: | **divides** | **does not divide**]

Because 82 mod 18= ___ 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)=_____

gcd(1226463,1)=_____

gcd(2498410,0)=_____

gcd(0,1226463)=_____

gcd(430586,430586)=_____

gcd(1,2498410)=_____

gcd(1226464,1226464)=_____

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)=___

gcd(7883,0)=___

gcd(7883,7884)=___

gcd(9271,9271)=___

Problem 4.2 (4) **(1 point)**

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

gcd(13,0)=_____

gcd(13,14)=_____

gcd(6,6)=_____

gcd(1,5)=_____

gcd(6,1)=_____

gcd(3,2)=_____

gcd(1,5)=_____

gcd(0,3)=_____

Problem 4.2 (5) **(1 point)**

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

gcd(15,16)=_____

gcd(10,1)=_____

gcd(29,0)=_____

gcd(0,10)=_____

gcd(7,7)=_____

gcd(1,29)=_____

gcd(11,10)=_____

Problem 4.2 (6) **(1 point)**

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

gcd(20,21)=_____

gcd(20,1)=_____

gcd(21,0)=_____

gcd(0,20)=_____

gcd(25,25)=_____

gcd(1,21)=_____

gcd(21,20)=_____

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 mod b,b) = [select: | **0** | **1** | **a** | **b** | **a+b** | **gcd(a,b)**]

gcd(a,0) = [select: | **0** | **1** | **a** | **b** | **a+b** | **gcd(a,b)**]

gcd(1,b) = [select: | **0** | **1** | **a** | **b** | **a+b** | **gcd(a,b)**]

gcd(b+1,b) = [select: | **0** | **1** | **a** | **b** | **a+b** | **gcd(a,b)**]

gcd(a-b,b) = [select: | **0** | **1** | **a** | **b** | **a+b** | **gcd(a,b)**]

a mod b < [select: | **0** | **1** | **a** | **b** | **a+b** | **gcd(a,b)**]

gcd(b,a) = [select: | **0** | **1** | **a** | **b** | **a+b** | **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 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
- 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 $r := a \bmod b =$ ___ and **let** $a := b =$ ___ and **let** $b := r =$ ___

let $r := a \bmod b =$ ___ and **let** $a := b =$ ___ and **let** $b := r =$ ___

The greatest common divisor of 52 and 24 is $a =$___

Problem 4.3 (2) **(1 point)**

Follow these step to compute the greatest common divisor of $a := 41$ and $b := 21$:

let $r := a \bmod b =$ ___ and **let** $a := b =$ ___ and **let** $b := r =$ ___

let $r := a \bmod b =$ ___ and **let** $a := b =$ ___ and **let** $b := r =$ ___

let $r := a \bmod b =$ ___ and **let** $a := b =$ ___ and **let** $b := r =$ ___

The greatest common divisor of 41 and 21 is $a =$___

Problem 4.3 (3) **(1 point)**

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

gcd(30,42)=___

gcd(105,165)=___

gcd(360,504)=___

Problem 4.3 (4) (1 point)

Compute these greatest common divisiors with the Euclidean Algorithm:

gcd(12, 34) = _____

gcd(28, 25) = _____

gcd(126, 216) = _____

gcd(119, 196) = _____

gcd(80, 100) = _____

gcd(264, 407) = _____

Problem 4.3 (5) (1 point)

Compute these greatest common divisiors with the Euclidean Algorithm:

gcd(23, 25) = _____

gcd(78, 93) = _____

gcd(275, 385) = _____

gcd(84, 189) = _____

gcd(319, 352) = _____

gcd(105, 238) = _____

Problem 4.3 (6) (1 point)

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

gcd(30,78)=_____

gcd(189189,189190)=_____

gcd(65,85)=___

gcd(798879,1)=_____

gcd(810277,0)=_____

gcd(10932,10932)=_____

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 $k := 24$? ___
What does the algorithm return when the input is $v := 128$ and $k := 24$? ___
What does the algorithm return when the input is $v := 87$ and $k := 24$? ___
What does the algorithm return when the input is $v := 30$ and $k := 24$? ___

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 ^ 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 mod h)**]

+

[select: | **(f*h)** | $(d+h)^2$ | **(f div h)** | **(d+h)** | $(f+h)^2$ | **(h-f)** | **(d*h)** | **(c*d)** | **(d-h)** | **(d+c)**]

=

[select: | **(f div h)** | **(f mod 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 $a_1 := b =$___ and let $b_1 := a \bmod b =$ ___ and let $q_1 := a \operatorname{div} b =$___

Let $a_2 := b_1$=___ and let $b_2 := a_1 \bmod b_1 =$ ___

We have computed $\gcd(147,70) = b_1 =$___.

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 (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 $a_1 := b =$___ and let $b_1 := a \bmod b =$ ___ and let $q_1 := a \operatorname{div} b =$___

Let $a_2 := b_1$=___ and let $b_2 := a_1 \bmod b_1 =$ ___

We have computed $\gcd(160, 30) = b_1 =$___.

Now write $a = (b \cdot q_1) + b_1$:

___ $= \left(\right.$___$\cdot$___$\left.\right) +$___

Rearranging the values, write $b_1 = (1 \cdot a) + ((-q_1) \cdot b)$:

___ $= \left(1 \cdot\right.$ ___$\left.\right) + \left(\right.$___$\cdot$___$\left.\right)$

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 (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 $a_1 := b =$___ and let $b_1 := a \bmod b =$ ___ and let $q_1 := a \operatorname{div} b =$___

Let $a_2 := b_1$=___ and let $b_2 := a_1 \bmod b_1 =$ ___

We have computed $\gcd(26, 6) = b_1 =$___.

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 $\underline{\quad (A) \quad}$ of distinct $\underline{\quad (B) \quad}$.

(A): [select: | **flock** | **pile** | **bucket** | **heap** | **collection** | **stack** | **pack** | **list**]

(B): [select: | **birds** | **bears** | **numbers** | **letters** | **words** | **objects**]

The $\underline{\quad (C) \quad}$ in a set are called $\underline{\quad (D) \quad}$ 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 $\underline{\quad (A) \quad}$ between $\underline{\quad (B) \quad}$.

(A): [select: | **commas** | **semicolons** | **colons** | **spaces**]

(B): [select: | **parenthesis** | **angle brackets** | **square brackets** | **curly brackets**]

This way of describing a set is called $\underline{\quad (C) \quad}$.
(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): $\{5,6,7,\ldots,14\} = \{$____________________$\}$

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 $\underline{\quad (A) \quad}$ 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 $\underline{\quad (B) \quad}$ 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 $\underline{\quad (C) \quad}$ the set B and write $A = B$ if each element in the set A $\underline{\quad (D) \quad}$ the set B and if each element in the set B $\underline{\quad (E) \quad}$ 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 $\underline{\quad (F) \quad}$ 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 $S = \{7, 8, 9, \ldots, 37\}$. 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 $A = \{43, 44, 45, ..., 50\}$.

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,...,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. $\{\ldots,-3,-2,-1,0,1,2,3,\ldots\}$
___ 2. $\mathbb{Z}_{16}$	B. the set that contains no elements
___ 3. $\mathbb{Z}$	C. $\{0,1,2,3,\ldots,15\}$

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. $\mathbb{Z}_6 = \{$____________________$\}$

Problem 5.4 (5) (1 point)

Give the set in roster form. $\mathbb{Z}_4^{\otimes} = \{$_____________________$\}$

Problem 5.4 (6) (1 point)

For each statement indicate whether it is true or false.

1. ___ $\texttt{r} \in \mathbb{A}$
2. ___ $\texttt{h} \in \mathbb{A}$
3. ___ $\texttt{5} \notin \mathbb{A}$
4. ___ $41 \in \{\}$
5. ___ $\texttt{a} \in \mathbb{A}$

Problem 5.4 (7) (1 point)

For each statement indicate whether it is true or false.

1. ___ $\texttt{8} \notin \mathbb{A}$
2. ___ $\{\} = \mathbb{Z}$
3. ___ $\texttt{z} \notin \mathbb{A}$
4. ___ $0 \in \mathbb{Z}_8^{\otimes}$

Problem 5.4 (8) (1 point)

For each statement indicate whether it is true or false.

1. ___ $\texttt{6} \notin \mathbb{A}$
2. ___ $65 \notin \mathbb{Z}_{63}$
3. ___ $0 \in \mathbb{Z}_6$
4. ___ $\texttt{6} \in \mathbb{A}$

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 mod 7 = _____

179 mod 4 = _____

176 mod 9 = _____

179 mod 13 = _____

169 mod 15 = _____

189 mod 11 = _____

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: $\mathbb{A} = \{-, \mathtt{a}, \mathtt{b}, \mathtt{c}, \ldots, \mathtt{z}\}$
$\mathbb{Z}_n = \{0, 1, 2, 3, \ldots, n-1\}$
$\mathbb{Z}_n^{\otimes} = \{1, 2, 3, \ldots, n-1\}$

Correct Answers:

- T
- F
- F
- F

Problem 5.4 (8) *Correct Answers:*

Hint: $\mathbb{A} = \{-, \mathtt{a}, \mathtt{b}, \mathtt{c}, \ldots, \mathtt{z}\}$
$\mathbb{Z}_n = \{0, 1, 2, 3, \ldots, n-1\}$
$\mathbb{Z}_n^{\otimes} = \{1, 2, 3, \ldots, n-1\}$

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 $\underline{\quad(A)\quad}$ a $\underline{\quad(B)\quad}$ a is $\underline{\quad(C)\quad}$ the set of $\underline{\quad(D)\quad}$ and a is $\underline{\quad(E)\quad}$ -6 and a is $\underline{\quad(F)\quad}$ -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.

$\{x \mid x \in \mathbb{Z} \text{ and } x > -3 \text{ and } x \leq 3\} = \{$ ____________________ $\}$

Problem 5.5 (3) **(1 point)**

Give the set in roster form (without ellipsis).

$\{x \mid x \in \mathbb{N} \text{ and } x \geq 27 \text{ and } x \leq 50 \text{ and } x \bmod 9 = 0\} = \{$____________________$\}$

Problem 5.5 (4) (1 point)

Give the set in roster form.

$\{x \mid x \in \mathbb{N} \text{ and } x < 17\} = \{$____________________$\}$

Problem 5.5 (5) (1 point)

Give the set in roster form.

$\{x \mid x \in \mathbb{N} \text{ and } x \leq 16 \text{ and } x \bmod 14 = 0\} = \{$____________________$\}$

[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

$(2+0^3) \bmod 5 =$ ___

$(2+1^3) \bmod 5 =$ ___

$(2+2^3) \bmod 5 =$ ___

$(2+3^3) \bmod 5 =$ ___

$(2+4^3) \bmod 5 =$ ___

Now find $\{(x, (2+x^3) \bmod 5) \mid x \in \mathbb{Z}_5\} = \{$____________________ $\} \subseteq \mathbb{Z}_5 \times \mathbb{Z}_5$.

Problem 5.5 (8) (1 point)

Give the set in roster form.

$\{x+18 \mid x \in \mathbb{Z} \text{ and } x \geq -7 \text{ and } x < 3\} = \{$ ____________________ $\}$

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. ___ $\{\} \in \{-2,3,7\}$
2. ___ $\{\} \subseteq \{-2,3,7\}$
3. ___ $\{\} \subseteq \{0\}$
4. ___ $\{\} \in \{\}$

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. ___ $C \subseteq D$

3. ___ $B \not\subseteq A$

4. ___ $A \subseteq B$

Problem 6.1 (7) (1 point)

For each statement indicate whether it is true or false.

1. ___ $\{0,1,2,\ldots,7\} \subseteq \mathbb{Z}_{23}^{\otimes}$
2. ___ $\mathbb{Z}_{23} \subseteq \{0,1,2,\ldots,23\}$
3. ___ $\mathbb{Z}_{19} \subseteq \{\}$
4. ___ $\{0\} \subseteq \{\}$

Problem 6.1 (8) (1 point)

Let $E = \{a,b,c,f,g\}$.

For each statement indicate whether it is true or false.

1. ___ $\{b,c,f\} \subseteq E$
2. ___ $\{a,b,c,f,g\} \subseteq E$
3. ___$\{c\} \subseteq E$
4. ___ $\{f,g\} \not\subseteq E$

Problem 6.1 (9) (1 point)

For each statement indicate whether it is true or false.

1. ___ $\{\,\} \subseteq \{\{\,\}\}$
2. ___ $\{\,\} \not\subseteq \{3,8,17,23\}$
3. ___ $\{\,\} \not\subseteq \{\,\}$
4. ___ $\{\{\,\}\} \subseteq \{\{\},\{\{\}\},0,1\}$

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 $B \nsubseteq A$ 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 div 7 = _____ and
9 mod 7 = _____

-48 div 22 = _____ and
-48 mod 22 = _____

17 div 14 = _____ and
17 mod 14 = _____

-45 div 28 = _____ and
-45 mod 28 = _____

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: $\mathbb{Z}_n = \{0, 1, 2, 3, \ldots, n-1\}$
$\mathbb{Z}_n^{\otimes} = \{1, 2, 3, \ldots, n-1\}$

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 $\underline{\quad (A) \quad}$ of the sets A and B, denoted by $A \times B$, is the set of all $\underline{\quad (B) \quad}$ (a,b) where a is $\underline{\quad (C) \quad}$ the set A $\underline{\quad (D) \quad}$ b is $\underline{\quad (E) \quad}$ 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 $A = \{7,8,9,\ldots,20\}$
Let $B = \{-6,-5,-4,\ldots,3\}$

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.

$A \times B = \{$______________________________$\}$

Problem 6.2 (5) (1 point)

Let $A = \{2,3,4,5\}$. Give the set in roster form.

$\{(a, 9 \cdot a) \mid a \in A\} = \{$______________________________$\}$

[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.

$\{(a, a \bmod 4) \mid a \in A\} = \{$______________________________$\}$

[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.

$A \times B = \{$______________________________$\}$

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:

$(a+a) \bmod 4$ = ___

$(a+b) \bmod 4$ = ___

$(a \cdot b) \bmod 4$ = ___

$(a+2) \bmod 4$ = ___

$(2 \cdot b) \bmod 4$ = ___

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:*

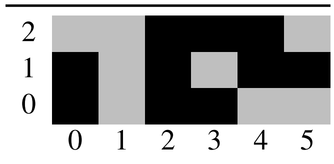
- $(10,1),(11,1),(12,1)$

Problem 6.2 (8) *Correct Answers:*

- 0
- 1
- 0
- 2
- 2

6.3 Applications of Cartesian Products

Problem 6.3 (1) (1 point)

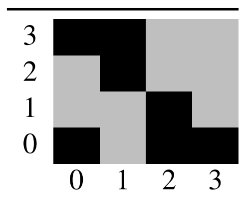


The subset of $\{0,1,2,3,4,5\} \times \{0,1,2\}$ represented by the black pixels in the raster above is:

{——————————}

[although it would be mathematically correct, answers with repeated elements will be marked as wrong]

Problem 6.3 (2) (1 point)

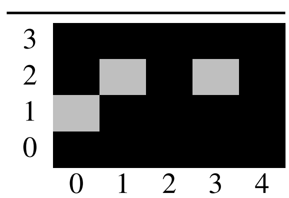


The subset of $\{0,1,2,3\} \times \{0,1,2,3\}$ represented by the black pixels in the raster above is:

{——————————}

[although it would be mathematically correct, answers with repeated elements will be marked as wrong]

Problem 6.3 (3) (1 point)

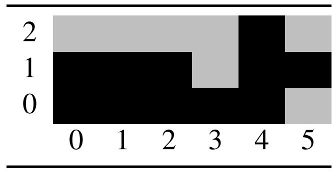


The subset of $\{0,1,2,3,4\} \times \{0,1,2,3\}$ represented by the black pixels in the raster above is:

{——————————}

[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 div 2 = _____ and
6 mod 2 = _____

-44 div 21 = _____ and
-44 mod 21 = _____

24 div 11 = _____ and
24 mod 11 = _____

-46 div 27 = _____ and
-46 mod 27 = _____

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 $\underline{\quad (A) \quad}$ of B to $\underline{\quad (B) \quad}$ 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 $\underline{\quad (C) \quad}$ of the function and the set B is called the $\underline{\quad (D) \quad}$ 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 $g : \mathbb{Z}_{16} \to \mathbb{Z}_{20}$. Identify the following:

1. ___ g
2. ___ $\mathbb{Z}_{16}$
3. ___ $g(11)$
4. ___ $\mathbb{Z}_{20}$

Problem 7.1 (3) (1 point)

Let $f : \mathbb{Z} \to \mathbb{Z}_8,\ f(x) = (x) \bmod 8$. Find:

$f(3) =$___

$f(-5) =$___

$f(16) =$___

Problem 7.1 (4) (1 point)

Let the function $k : \mathbb{Z}_9 \to \mathbb{Z}_7$ be given by $k(x) = (1+x^3) \bmod 7$.

Find k evaluated at all elements of its domain.

$k(0) =$ ___

$k(1) =$ ___

$k(2) =$ ___

$k(3) =$ ___

$k(4) =$ ___

$k(5) =$ ___

$k(6) =$ ___

$k(7) =$ ___

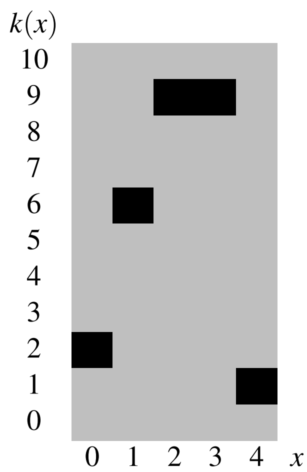
$k(8) =$ ___

In roster form the image of A under k is $\{k(x) \mid x \in \mathbb{Z}_9\} = \{$____________________$\}$.

In roster form the graph of k is $\{(x, k(x)) \mid x \in \mathbb{Z}_9\} = \{$____________________$\}$.

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 $\{$____________________$\}$.

In roster form the domain of k is $A = \{$ ____________________ $\}$.

In roster form the codomain of k is $B = \{$ ____________________ $\}$.

Find k evaluated at all elements of its domain.

$k(0) =$ ___

$k(1) =$ ___

$k(2) =$ ___

$k(3) =$ ___

$k(4) =$ ___

In roster form the image of A under k is $\{k(x) \mid x \in A\} = \{$____________________ $\}$.

Problem 7.1 (7) (1 point)

Consider the function $G : \mathbb{Z} \to \mathbb{Z}$ defined by $G(x) = -2x^2 - 3x + 3$.

Evaluate the following:

a. $G(0) =$ _____

b. $G(-2) =$ _____

Problem 7.1 (8) **(1 point)**

Let $S := \{-10, -5, 0, 5, 10\}$ and let $g : S \to S$ 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)

$g(0) =$ ___

$g(5) =$ ___

$g($ ___ $) = 0$

$g($ ___ $) = 5$

Problem 7.1 (9) **(1 point)**

Consider the function

$g : \{-2, -1, ..., 6, 7\} \to \{-2, -1, ..., 6, 7\}$

x	-2	-1	0	1	2	3	4	5	6	7
$g(x)$	6	0	4	5	2	-2	1	-1	3	6

Find $g(-2)$.
$g(-2) =$___

Problem 7.1 (10) **(1 point)**

Let $f : \mathbb{Z}_3 \to \mathbb{Z}_3,\ f(x) = (0) \bmod 3$.

Evaluate f at all elements of the domain:

$f(0) =$ ___

$f(1) =$ ___

$f(2) =$ ___

Problem 7.1 (11) (1 point)

Let the function $h : \mathbb{Z}_7 \to \mathbb{Z}_5$ be given by $h(x) = (4 \cdot x) \bmod 5$.

Find h evaluated at all elements of its domain.

$h(0) =$ ___

$h(1) =$ ___

$h(2) =$ ___

$h(3) =$ ___

$h(4) =$ ___

$h(5) =$ ___

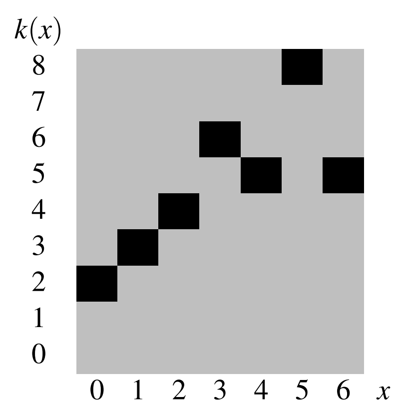
$h(6) =$ ___

In roster form the image of A under h is $\{h(x) \mid x \in \mathbb{Z}_7\} = \{$____________________$\}$.

In roster form the graph of h is $\{(x, h(x)) \mid x \in \mathbb{Z}_7\} = \{$____________________$\}$.

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 $\{(x, k(x)) \mid x \in A\} = \{$____________________$\}$.

In roster form the domain of k is $A = \{$ ____________________ $\}$.

In roster form the codomain of k is $B = \{$ ____________________ $\}$.

In roster form the image of A under k is $\{k(x) \mid x \in A\} = \{$____________________$\}$.

Find k evaluated at all elements of its domain.

$k(0) =$ ___

$k(1) =$ ___

$k(2) =$ ___

$k(3) =$ ___

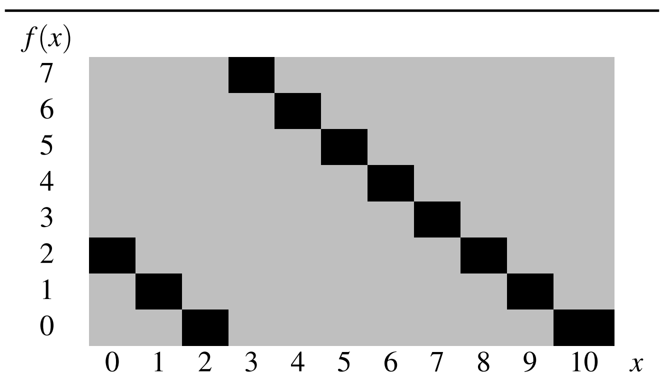
$k(4) =$ ___

$k(5) =$ ___

$k(6) =$ ___

Problem 7.1 (13) (1 point)

Suppose that the graph of the function f is



In roster form the domain of f is $A = \{$ ____________________ $\}$.

In roster form the codomain of f is $B = \{$ ____________________ $\}$.

In roster form the image of A under f is $\{f(x) \mid x \in A\} = \{$____________________$\}$.

Find f evaluated at all elements of its domain.

$f(0) =$ ___

$f(1) =$ ___

$f(2) = \_\_\_$

$f(3) = \_\_\_$

$f(4) = \_\_\_$

$f(5) = \_\_\_$

$f(6) = \_\_\_$

$f(7) = \_\_\_$

$f(8) = \_\_\_$

$f(9) = \_\_\_$

$f(10) = \_\_\_$

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:

$\{k(x) \mid x \in \mathbb{Z}_9\} = \{k(x) \mid x \in \{0,1,\ldots,9\} = \{k(0),k(1),\ldots,k(8)\} = \{1,2,\ldots,2\}$

The graph of k is:

$\{(x,k(x)) \mid x \in \mathbb{Z}_9\} = \{(x,k(x)) \mid x \in \{0,1,2,\ldots,8\}\} = \{(0,k(0)),(1,k(1)),\ldots,(8,k(8))\} = \{(0,1),(1,2),\ldots,(8,2)\}$

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 $\{0,1,\ldots,4\} \times \{0,1,\ldots,10\}$ that is represented by black pixels. Thus the graph of k is

$\{(0,2),(1,6),\ldots,(4,1)\}$

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 of the values of k evaluated at the elements of the domain from the graph and get:

$k(0) = 6$, $k(1) = 6$, 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:

$\{k(x) \mid x \in \{0,1,\ldots,4\} = \{k(0),k(1),\ldots,k(4)\} = \{2,6,\ldots,1\}$

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. $$\begin{aligned} G(0) &= -2(0)^2 - 3(0) + 3 \\ &= -2(0) + 0 + 3 \\ &= 0 + 0 + 3 \\ &= 3 \end{aligned}$$

b. $$\begin{aligned} G(-2) &= -2(-2)^2 - 3(-2) + 3 \\ &= -2(4) + 6 + 3 \\ &= -8 + 6 + 3 \\ &= 1 \end{aligned}$$

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 $k : A \to B$ 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 $f : A \to B$ 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 $f : A \to B$ and $g : A \to B$ be functions.

We say that f and g $\underline{\ \ (A)\ \ }$ and write $f = g$ if $\underline{\ \ (B)\ \ }$ 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 $\underline{\ \ (C)\ \ }$, 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

$f : \mathbb{Z}_8 \to \mathbb{Z}_8,\ f(x) = (x+2) \bmod 8$ and

$g : \mathbb{Z}_8 \to \mathbb{Z}_8,\ g(x) = (x-6) \bmod 8$

are equal, evaluate them at all points of their domain:

$f(0) =$ ___ $g(0) =$ ___

$f(1) =$ ___ $g(1) =$ ___

$f(2) =$ ___ $g(2) =$ ___

$f(3) =$ ___ $g(3) =$ ___

$f(4) =$ ___ $g(4) =$ ___

$f(5) =$ ___ $g(5) =$ ___

$f(6) = \_\_\_$ $g(6) = \_\_\_$

$f(7) = \_\_\_$ $g(7) = \_\_\_$

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

$f : \mathbb{Z}_5 \to \mathbb{Z}_5,\ f(x) = (1 \cdot x) \bmod 5$ and

$g : \mathbb{Z}_5 \to \mathbb{Z}_5,\ g(x) = (2 \cdot x) \bmod 5$

are equal, evaluate them at all points of their domain:

$f(0) = \_\_\_$ $g(0) = \_\_\_$

$f(1) = \_\_\_$ $g(1) = \_\_\_$

$f(2) = \_\_\_$ $g(2) = \_\_\_$

$f(3) = \_\_\_$ $g(3) = \_\_\_$

$f(4) = \_\_\_$ $g(4) = \_\_\_$

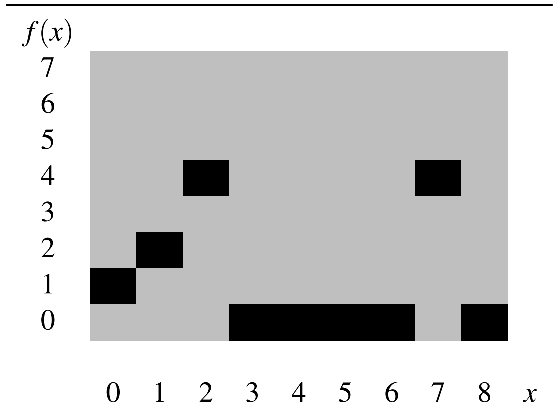
Now conclude whether they are equal.

The function f ______________ the function g.

[select: | **is equal to** | **is not equal to**]

Problem 7.2 (4) (1 point)

Let $f : \mathbb{Z}_9 \to \mathbb{Z}_8,$ be given by



Let $g : \mathbb{Z}_9 \to \mathbb{Z}_8,\ g(x) = 2^x \mod 8$.
To determine whether the functions f and g are equal find:

$f(0) =$ ___ $g(0) =$ ___

$f(1) =$ ___ $g(1) =$ ___

$f(2) =$ ___ $g(2) =$ ___

$f(3) =$ ___ $g(3) =$ ___

$f(4) =$ ___ $g(4) =$ ___

$f(5) =$ ___ $g(5) =$ ___

$f(6) =$ ___ $g(6) =$ ___

$f(7) =$ ___ $g(7) =$ ___

$f(8) =$ ___ $g(8) =$ ___

Now conclude whether f and g are equal.

The function f $\underline{\ \ (A)\ \ }$ the function g, because $f(x)$ $\underline{\ \ (B)\ \ }$ $g(x)$ for $\underline{\ \ (C)\ \ }$.

(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

$f : \mathbb{Z}_4 \to \mathbb{Z}_4,\ f(x) = (x+1) \bmod 4$ and

$g : \mathbb{Z}_4 \to \mathbb{Z}_4,\ g(x) = (x-1) \bmod 4$

are equal, evaluate them at all points of their domain:

$f(0) = \_\_\_$ $g(0) = \_\_\_$

$f(1) = \_\_\_$ $g(1) = \_\_\_$

$f(2) = \_\_\_$ $g(2) = \_\_\_$

$f(3) = \_\_\_$ $g(3) = \_\_\_$

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

$f : \mathbb{Z}_7 \to \mathbb{Z}_7,\ f(x) = (1 \cdot x) \bmod 7$ and

$g : \mathbb{Z}_7 \to \mathbb{Z}_7,\ g(x) = (2 \cdot x) \bmod 7$

are equal, evaluate them at all points of their domain:

$f(0) = \_\_\_$ $g(0) = \_\_\_$

$f(1) = \_\_\_$ $g(1) = \_\_\_$

$f(2) = \_\_\_$ $g(2) = \_\_\_$

$f(3) = \_\_\_$ $g(3) = \_\_\_$

$f(4) = \_\_\_$ $g(4) = \_\_\_$

$f(5) = \_\_\_$ $g(5) = \_\_\_$

$f(6) = \_\_\_\quad g(6) = \_\_\_$

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

$f : \mathbb{Z}_3^{\otimes} \to \mathbb{Z}_3^{\otimes},\ f(x) = x^2$ mod 3 and

$g : \mathbb{Z}_3^{\otimes} \to \mathbb{Z}_3^{\otimes},\ g(x) = 1$

are equal, evaluate them at all points of their domain:

$f(1) = \_\_\_\quad g(1) = \_\_\_$

$f(2) = \_\_\_\quad g(2) = \_\_\_$

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. ___ $f : \mathbb{Z}_5 \to \mathbb{Z}_5,\ f(x) = (x+1)$ mod 5 and $g : \mathbb{Z}_5 \to \mathbb{Z}_5,\ g(x) = (x-4)$ mod 5
2. ___ $f : \mathbb{Z} \to \mathbb{Z},\ f(x) = x+1$ and $g : \mathbb{Z} \to \mathbb{Z},\ g(x) = x-4$
3. ___ $f : \mathbb{Z}_{10} \to \mathbb{Z}_{10},\ f(x) = (x+3)$ mod 10 and $g : \mathbb{Z}_{10} \to \mathbb{Z}_{10},\ g(x) = (x-3)$ mod 10
4. ___ $f : \mathbb{Z}_3 \to \mathbb{Z}_3,\ f(x) = x^2$ mod 3 and $g : \mathbb{Z}_3 \to \mathbb{Z}_3,\ g(x) = x$

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 $f : A \to B$ 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 $f : A \to B$ and $g : A \to B$ 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
- 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 → C and g : A → B be functions.

The $\underline{\quad (A) \quad}$ of f and g, written f∘g, is the function f∘g : $\underline{\quad (B) \quad}$ → $\underline{\quad (C) \quad}$ defined by f∘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

$f : \mathbb{Z}_3 \to \mathbb{Z}_3$, $f(x) = (x+1) \bmod 3$

and

$g : \mathbb{Z} \to \mathbb{Z}_3$, $g(x) = (0) \bmod 3$.

Evaluate:

$g(0) =$ ___ $f(g(0)) =$ ___

$g(1) =$ ___ $f(g(1)) =$ ___

$g(2) =$ ___ $f(g(2)) =$ ___

Problem 7.3 (3) (1 point)

Consider the two functions

$f : \mathbb{Z}_5 \to \mathbb{Z}_5$, $f(x) = (x^5 + 4) \bmod 5$

and

$g : \mathbb{Z} \to \mathbb{Z}_5$, $g(x) = (4x^2 + 3x) \bmod 5$.

Evaluate:

$g(0) = \_\_\_$ $f(g(0)) = \_\_\_$

$g(1) = \_\_\_$ $f(g(1)) = \_\_\_$

$g(2) = \_\_\_$ $f(g(2)) = \_\_\_$

$g(3) = \_\_\_$ $f(g(3)) = \_\_\_$

$g(4) = \_\_\_$ $f(g(4)) = \_\_\_$

Problem 7.3 (4) (1 point)

Consider the two functions

$h : \mathbb{Z}_6 \to \mathbb{Z}_2$ given by $h(x) = ((1 \cdot x^2) + 0) \bmod 2$

and

$m : \mathbb{Z}_6 \to \mathbb{Z}_6$ given by $m(x) = ((1 \cdot x^2) + 5) \bmod 6$.

Evaluate:

$m(0) = \_\_\_$ $(h \circ m)(0) = \_\_\_$

$m(1) = \_\_\_$ $(h \circ m)(1) = \_\_\_$

$m(2) = \_\_\_$ $(h \circ m)(2) = \_\_\_$

$m(3) = \_\_\_$ $(h \circ m)(3) = \_\_\_$

$m(4) = \_\_\_$ $(h \circ m)(4) = \_\_\_$

$m(5) = \_\_\_$ $(h \circ m)(5) = \_\_\_$

Problem 7.3 (5) (1 point)

Consider the two functions

$g : \mathbb{Z}_4 \to \mathbb{Z}_4$ given by $g(x) = (3x + 2) \bmod 4$

and

$h : \mathbb{Z}_4 \to \mathbb{Z}_4$ given by $h(x) = (3) \bmod 4$.

Let $f := g \circ h$.

Evaluate:

$f(0) =$ ___

$f(1) =$ ___

$f(2) =$ ___

$f(3) =$ ___

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:

$(f \circ g)(3) =$ ___ $f(g(3)) =$ ___

$(g \circ f)(0) =$ ___ $g(f(0)) =$ ___

$(h \circ h)(2) =$ ___ $h(h(2)) =$ ___

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 $id_A : A \to A$ given by $id_A(x) =$ ______.

[select: | **?** | **0** | **1** | **-1** | **x** | **-x** | $\frac{1}{x}$ | $-\frac{1}{x}$]

Let B be a set and $f : A \to B$ and $g : B \to A$ be functions.

Then (f ∘ $id_A(x)$) = ______.

[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 ∘ g)(x) = ______.

[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 mod 4 = ___

1 mod 4 = ___

2 mod 4 = ___

3 mod 4 = ___

4 mod 4 = ___

5 mod 4 = ___

6 mod 4 = ___

7 mod 4 = ___

8 mod 4 = ___

9 mod 4 = ___

Problem 7.4 (3) **(1 point)**

Let $f : \mathbb{Z}_7 \to \mathbb{Z}_7$ be given by $f(x) = \left(3x^6 + 6x^4\right) \bmod 7$.

Let $\mathrm{id}_{\mathbb{Z}_7} : \mathbb{Z}_7 \to \mathbb{Z}_7$ given by $\mathrm{id}_{\mathbb{Z}_7}(x) = x$ be the identity function on $\mathbb{Z}_7$.

Evaluate f and $\mathrm{id}_{\mathbb{Z}_7}$ at all elements of the domain:

$f(0) =$ ___ $\mathrm{id}_{\mathbb{Z}_7}(0) =$ ___

$f(1) =$ ___ $\mathrm{id}_{\mathbb{Z}_7}(1) =$ ___

$f(2) =$ ___ $\mathrm{id}_{\mathbb{Z}_7}(2) =$ ___

$f(3) =$ ___ $\mathrm{id}_{\mathbb{Z}_7}(3) =$ ___

$f(4) =$ ___ $\mathrm{id}_{\mathbb{Z}_7}(4) =$ ___

$f(5) =$ ___ $\mathrm{id}_{\mathbb{Z}_7}(5) =$ ___

$f(6) =$ ___ $\mathrm{id}_{\mathbb{Z}_7}(6) =$ ___

Now determine whether f is equal to $\mathrm{id}_{\mathbb{Z}_7}$.

The function f _____ to $\mathrm{id}_{\mathbb{Z}_7}$.

[select: | **is equal** | **is NOT equal**]

Problem 7.4 (4) **(1 point)**

Let $f : \mathbb{Z}_5 \to \mathbb{Z}_5,\ f(x) = \left(4x^3 + 2x\right) \bmod 5$.

Evaluate f at all elements of the domain:

$f(0) =$ ___ $\mathrm{id}_{\mathbb{Z}_5}(0) = 0$

$f(1) =$ ___ $\mathrm{id}_{\mathbb{Z}_5}(1) = 1$

$f(2) =$ ___ $\mathrm{id}_{\mathbb{Z}_5}(2) = 2$

$f(3) =$ ___ $\mathrm{id}_{\mathbb{Z}_5}(3) = 3$

$f(4) =$ ___ $\mathrm{id}_{\mathbb{Z}_5}(4) = 4$

Now determine whether f is equal to the identity function $id_{\mathbb{Z}_5}$. For you 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 $f : \mathbb{Z}_3 \to \mathbb{Z}_3,\ f(x) = \left(x^2\right) \bmod 3.$

Evaluate f at all elements of the domain:

$f(0) =$ ___

$f(1) =$ ___

$f(2) =$ ___

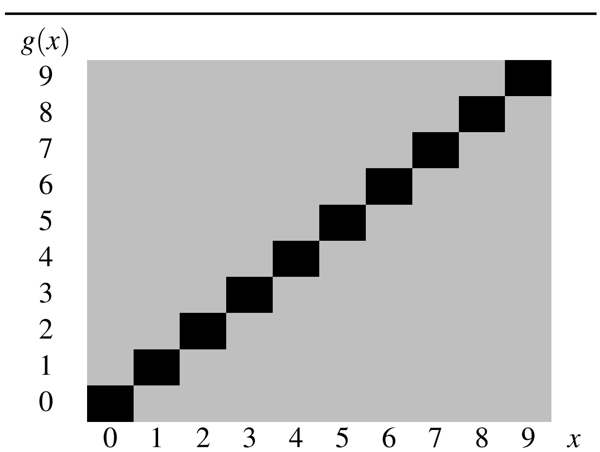
Now conclude whether f is equal to the identity function on $\mathbb{Z}_3$.

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 $A = \{$ ____________________ $\}$.

In roster form the codomain of g is $B = \{$ ______________________ $\}$.

In roster form the image of A under g is $\{g(x) \mid x \in A\} = \{$______________________ $\}$.

Find g evaluated at all elements of its domain.

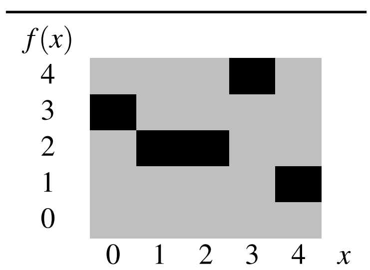
$g(0) =$ ___
$g(1) =$ ___
$g(2) =$ ___
$g(3) =$ ___
$g(4) =$ ___
$g(5) =$ ___
$g(6) =$ ___
$g(7) =$ ___
$g(8) =$ ___
$g(9) =$ ___

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 $A = \{$ ______________________ $\}$.

In roster form the codomain of f is $B = \{$ ______________________ $\}$.

In roster form the image of A under f is $\{f(x) \mid x \in A\} = \{$______________________ $\}$.

Find f evaluated at all elements of its domain.

$f(0) =$ ___
$f(1) =$ ___
$f(2) =$ ___
$f(3) =$ ___

$f(4) =$ ___

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 $g : A \to B$ 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 $f : A \to B$ 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 $f : A \to B$ be a function.

We say f is invertible if $\underline{\quad (A) \quad}$ element $\underline{\quad (B) \quad}$, $\underline{\quad (C) \quad}$ element $\underline{\quad (D) \quad}$ such that $\underline{\quad (E) \quad}$.

(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 $f^{-1} : \underline{\quad (A) \quad}$ of an invertible function $f : A \to B$ is the function that assigns to each element $\underline{\quad (B) \quad}$ the unique element $\underline{\quad (C) \quad}$ such that $\underline{\quad (D) \quad}$.

(A): [select: | $A \to B$ | $B \to A$]

(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 $f : \underline{\qquad}$ is invertible and $f^{-1} : B \to A$ is its inverse, then f is the inverse of f^{-1}.

[select: | $A \to B$ | $B \to A$]

Theorem. Let $f : A \to B$ be a function and let f^{-1} : $\underline{\quad (A) \quad}$ be its inverse, The function $f \circ f^{-1}$ is the $\underline{\quad (B) \quad}$. The function $f^{-1} \circ f$ is the $\underline{\quad (C) \quad}$.

(A): [select: | $A \to B$ | $B \to A$]

(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 $g : \{8, 9, ..., 16, 17\} \to \{8, 9, ..., 16, 17\}$ 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.
$g^{-1}(17) =$___

Problem 7.5 (3) (1 point)

Consider the function

$\varphi : \{-8, -7, ..., 0, 1\} \to \{-8, -7, ..., 0, 1\}$

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 $f^{-1}(5) =$ ___.

If $f^{-1}(-5) = -9$ then $f(-9) =$ ___.

Problem 7.5 (5) (1 point)

Let $f : \mathbb{Z}_2 \to \mathbb{Z}_2$, $f(x) = (x) \bmod 2$.

Evaluate f at all elements of its domain.

$f(0) =$ ___

$f(1) =$ ___

Thus the function f _____.

[select: | **is invertible** | **is not invertible**]

Problem 7.5 (6) (1 point)

Consider the function $g : \{-3, -2, ..., 5, 6\} \to \{-3, -2, ..., 5, 6\}$ 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 ? ___ (Y or N)

Problem 7.5 (7) (1 point)

Let $f : \mathbb{Z}_{11} \to \mathbb{Z}_{11},\ f(x) = (6x) \bmod 11$. Evaluate f at all elements of the domain:

$f(0) =$ ___

$f(1) =$ ___

$f(2) =$ ___

$f(3) =$ ___

$f(4) =$ ___

$f(5) =$ ___

$f(6) =$ ___

$f(7) = \_\_$

$f(8) = \_\_$

$f(9) = \_\_$

$f(10) = \_\_$

The function f is invertible. Find the image of the inverse f^{-1} of f at all elements of its domain.

$f^{-1}(0) = \_\_$

$f^{-1}(1) = \_\_$

$f^{-1}(2) = \_\_$

$f^{-1}(3) = \_\_$

$f^{-1}(4) = \_\_$

$f^{-1}(5) = \_\_$

$f^{-1}(6) = \_\_$

$f^{-1}(7) = \_\_$

$f^{-1}(8) = \_\_$

$f^{-1}(9) = \_\_$

$f^{-1}(10) = \_\_$

Problem 7.5 (8) (1 point)

Let $f : \mathbb{Z}_6 \to \mathbb{Z}_6,\ f(x) = (1+x) \bmod 6$.

Evaluate f at all elements of the domain:

$f(0) = \_\_$

$f(1) = \_\_$

$f(2) = \_\_$

$f(3) = \_\_$

$f(4) =$ ___

$f(5) =$ ___

The function f is invertible. Find the image of the inverse f^{-1} of f at all elements of its domain.

$f^{-1}(0) =$ ___

$f^{-1}(1) =$ ___

$f^{-1}(2) =$ ___

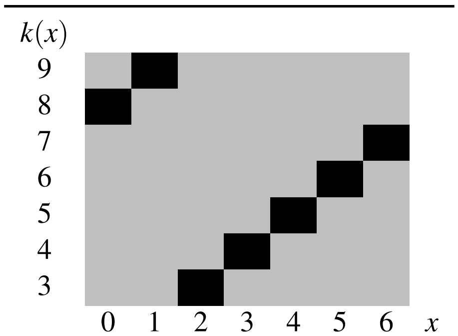
$f^{-1}(3) =$ ___

$f^{-1}(4) =$ ___

$f^{-1}(5) =$ ___

Problem 7.5 (9) (1 point)

Suppose that the graph of the function k is



In roster form the domain of k is $A = \{$ ____________________ $\}$.

In roster form the codomain of k is $B = \{$ ____________________ $\}$.

Find k evaluated at all elements of its domain.

$k(0) =$ ___
$k(1) =$ ___
$k(2) =$ ___
$k(3) =$ ___
$k(4) =$ ___
$k(5) =$ ___

$k(6) =$ ___

In roster form the image of A under k is $\{k(x) \mid x \in A\} = \{$____________________$\}$.

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 { ____________________ }.

In roster form the codomain of k^{-1} is { ____________________ }.

Give the preimages of all elements of the codomain.

$k^{-1}(3) =$ ___
$k^{-1}(4) =$ ___
$k^{-1}(5) =$ ___
$k^{-1}(6) =$ ___
$k^{-1}(7) =$ ___
$k^{-1}(8) =$ ___
$k^{-1}(9) =$ ___

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. ___ $f : \mathbb{Z}_5 \to \mathbb{Z}_5,\ f(x) = (x+2) \bmod 5$
2. ___ $f : \mathbb{Z}_{10} \to \mathbb{Z}_{10},\ f(x) = (2 \cdot x) \bmod 10$
3. ___ $f : \mathbb{Z}_7 \to \mathbb{Z}_7,\ f(x) = (x^3) \bmod 7$
4. ___ $f : \mathbb{Z}_5 \to \mathbb{Z}_5,\ f(x) = (x^3) \bmod 5$

Problem 7.5 (11) (1 point)

Let $S := \{1,2,3,4,5\}$ and let $g : S \to S$ 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)

$g(3) =$ ___

$g(2) =$ ___

$g^{-1}(3) =$ ___

$g^{-1}(2) =$ ___

Solutions

Problem 7.5 (1) *Correct Answers:*

- for every
- b in B
- there is exactly one
- a in A
- f(a)=b
- $B \to A$
- b in B
- a in A
- f(a)=b
- $A \to B$
- $B \to A$
- 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 $k : A \to B$ 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

8.1 Character Encoding

Problem 8.1 (1) (1 point)

We encode sequences of characters with the function

$$C : \{-, \mathtt{a}, \mathtt{b}, \mathtt{c}, ..., \mathtt{z}\} \to \{0, 1, 2, 3, ...26\}, C(-) = 0, C(\mathtt{a}) = 1, ..., C(\mathtt{z}) = 26.$$

Decode the sequence of integers into a string using the inverse of the endcoding function C:

$$20, 18, 1, 9, 20, 15, 18$$

Problem 8.1 (2) (1 point)

Let

$$C : \{-, \mathtt{a}, \mathtt{b}, \mathtt{c}, ..., \mathtt{z}\} \to \{0, 1, 2, 3, ...26\}, C(-) = 0, C(\mathtt{a}) = 1, ..., C(\mathtt{z}) = 26.$$

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

$$C : \{-, \mathtt{a}, \mathtt{b}, \mathtt{c}, ..., \mathtt{z}\} \to \{0, 1, 2, 3, ...26\}, C(-) = 0, C(\mathtt{a}) = 1, ..., C(\mathtt{z}) = 26.$$

Decode the sequence of integers into a string using the inverse of the endcoding function C:

$$19, 16, 1, 3, 5$$

Problem 8.1 (4) (1 point)

Let

$$C : \{-, \mathtt{a}, \mathtt{b}, \mathtt{c}, ..., \mathtt{z}\} \to \{0, 1, 2, 3, ...26\}, C(-) = 0, C(\mathtt{a}) = 1, ..., C(\mathtt{z}) = 26.$$

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

$$C : \{-, \mathtt{a}, \mathtt{b}, \mathtt{c}, ..., \mathtt{z}\} \to \{0, 1, 2, 3, ...26\}, C(-) = 0, C(\mathtt{a}) = 1, ..., C(\mathtt{z}) = 26.$$

Decode the sequence of integers into a string using the inverse of the endcoding function C:

$$1, 12, 5, 18, 20$$

____

Problem 8.1 (6) (1 point)

Let

$$C : \{-, \mathtt{a}, \mathtt{b}, \mathtt{c}, ..., \mathtt{z}\} \to \{0, 1, 2, 3, ...26\}, C(-) = 0, C(\mathtt{a}) = 1, ..., C(\mathtt{z}) = 26.$$

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 div 3 = ___

55 mod 3 = ___

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:

$\underline{\quad (A) \quad}$ sends a message to $\underline{\quad (B) \quad}$.

(A): [select: | **Alice** | **Bob** | **Eve** | **Oscar**]

(B): [select: | **Alice** | **Bob** | **Eve** | **Oscar**]

$\underline{\quad (C) \quad}$ eavesdrops on the communication between $\underline{\quad (D) \quad}$ and $\underline{\quad (E) \quad}$

(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 $\underline{\quad (A) \quad}$ and $\underline{\quad (B) \quad}$ 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**]

$\underline{\quad (C) \quad}$ encrypts a message using the encryption method and the key. She sends the encrypted message to $\underline{\quad (D) \quad}$.

(C): [select: | **Alice** | **Bob** | **Eve** | **Oscar**]

(D): [select: | **Alice** | **Bob** | **Eve** | **Oscar**]

$\underline{\quad (E) \quad}$ receives the message from $\underline{\quad (F) \quad}$ 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 = _____ and
89470 mod 1256 = _____

87435 div 2349 = _____ and
87435 mod 2349 = _____

61352 div 1845 = _____ and
61352 mod 1845 = _____

5687 div 2960 = _____ and
5687 mod 2960 = _____

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 $-$.

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 $D : \mathbb{A} \to \mathbb{A}$ given by

$D(-) =$___,
$D(\mathtt{a}) =$___,
$D(\mathtt{b}) =$___,
$D(\mathtt{c}) =$___,
$D(\mathtt{d}) =$___,
$D(\mathtt{e}) =$___,
$D(\mathtt{f}) =$___,
$D(\mathtt{g}) =$___,
$D(\mathtt{h}) =$___,
$D(\mathtt{i}) =$___,
$D(\mathtt{j}) =$___,
$D(\mathtt{k}) =$___,
$D(\mathtt{l}) =$___,
$D(\mathtt{m}) =$___,
$D(\mathtt{n}) =$___,
$D(\mathtt{o}) =$___,
$D(\mathtt{p}) =$___,
$D(\mathtt{q}) =$___,
$D(\mathtt{r}) =$___,
$D(\mathtt{s}) =$___,
$D(\mathtt{t}) =$___,
$D(\mathtt{u}) =$___,
$D(\mathtt{v}) =$___,
$D(\mathtt{w}) =$___,
$D(\mathtt{x}) =$___,
$D(\mathtt{y}) =$___,
$D(\mathtt{z}) =$___,

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 $E : \mathbb{A} \to \mathbb{A}$ given by:
$E(-) =$___,
$E(\mathtt{a}) =$___,
$E(\mathtt{b}) =$___,
$E(\mathtt{c}) =$___,
$E(\mathtt{d}) =$___,
$E(\mathtt{e}) =$___,
$E(\mathtt{f}) =$___,
$E(\mathtt{g}) =$___,
$E(\mathtt{h}) =$___,
$E(\mathtt{i}) =$___,
$E(\mathtt{j}) =$___,
$E(\mathtt{k}) =$___,
$E(\mathtt{l}) =$___,
$E(\mathtt{m}) =$___,
$E(\mathtt{n}) =$___,
$E(\mathtt{o}) =$___,
$E(\mathtt{p}) =$___,
$E(\mathtt{q}) =$___,
$E(\mathtt{r}) =$___,
$E(\mathtt{s}) =$___,
$E(\mathtt{t}) =$___,
$E(\mathtt{u}) =$___,
$E(\mathtt{v}) =$___,
$E(\mathtt{w}) =$___,
$E(\mathtt{x}) =$___,
$E(\mathtt{y}) =$___,
$E(\mathtt{z}) =$___,

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 div 50 = ___

35 mod 50 = ___

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 $f : \mathbb{Z}_4 \to \mathbb{Z}_4,\ f(x) = (2+x) \bmod 4$.

Evaluate f at all elements of the domain:

$f(0) =$ ___

$f(1) =$ ___

$f(2) =$ ___

$f(3) =$ ___

The function f is invertible. Find the image of the inverse f^{-1} of f at all elements of its domain.

$f^{-1}(0) =$ ___

$f^{-1}(1) =$ ___

$f^{-1}(2) =$ ___

$f^{-1}(3) =$ ___

Problem 8.4 (2) (1 point)

Bob receives an encrypted message from Alice:

`htklslxfkx`

First he applies the encoding function

$$C : \{-, \mathtt{a}, \mathtt{b}, \mathtt{c}, ..., \mathtt{z}\} \to \{0, 1, 2, 3, ...26\}, C(-) = 0, C(\mathtt{a}) = 1, ..., C(\mathtt{z}) = 26.$$

to each character of the encrypted message and obtains a sequence of integers:

____

Then Bob applies the decryption function

$$D : \{0, 1, 2, 3, ...26\} \to \{0, 1, 2, 3, ...26\},\ D(x) = (x - 19) \bmod 27.$$

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

$$C : \{-, \mathtt{a}, \mathtt{b}, \mathtt{c}, ..., \mathtt{z}\} \to \{0, 1, 2, 3, ...26\}, C(-) = 0, C(\mathtt{a}) = 1, ..., C(\mathtt{z}) = 26.$$

She obtains a sequence of integers:

____

Then Alice encrypts the message using the encryption function

$$E : \{0, 1, 2, 3, ...26\} \to \{0, 1, 2, 3, ...26\} E(x) = (x + 14) \bmod 27.$$

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

$$C : \{-, \mathtt{a}, \mathtt{b}, \mathtt{c}, ..., \mathtt{z}\} \to \{0, 1, 2, 3, ...26\}, C(-) = 0, C(\mathtt{a}) = 1, ..., C(\mathtt{z}) = 26.$$

to map characters to integers and to use the function

$$E : \{0, 1, 2, 3, ...26\} \to \{0, 1, 2, 3, ...26\}, E(x) = (x + 18) \bmod 27$$

for encryption. The inverse of the function E is

$$E^{-1} : \{0, 1, 2, ..., 26\} \to \{0, 1, 2, ..., 26\}, E^{-1}(x) = (x - 18) \bmod 27$$

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:

$C(\mathtt{t}) =$ ___, $C(\mathtt{o}) =$ ___, $C(\mathtt{a}) =$ ___, $C(\mathtt{d}) =$ ___.

She encrypts these with the function E and gets

$E(C(\mathtt{t})) =$ ___, $E(C(\mathtt{o})) =$ ___, $E(C(\mathtt{a})) =$ ___, $E(C(\mathtt{d})) =$ ___.

Alice sends these integers to Bob.

Bob receives the message and evaluates the function E^{-1} at the integers send by Alice:

$E^{-1}(E(C(\mathtt{t}))) =$ ___, $E^{-1}(E(C(\mathtt{o}))) =$ ___, $E^{-1}(E(C(\mathtt{a}))) =$ ___, $E^{-1}(E(C(\mathtt{d}))) =$ ___.

An application of C^{-1} yields:

$C^{-1}(E^{-1}(E(C(\mathtt{t})))) =$ ___, $C^{-1}(E^{-1}(E(C(\mathtt{o})))) =$ ___, $C^{-1}(E^{-1}(E(C(\mathtt{a})))) =$ ___, $C^{-1}(E^{-1}(E(C(\mathtt{d})))) =$ ___.

Problem 8.4 (5) (1 point)

Alice and Bob meet and agree to use the code

$$C : \{-, \mathtt{a}, \mathtt{b}, \mathtt{c}, ..., \mathtt{z}\} \to \{0, 1, 2, 3, ...26\}, C(-) = 0, C(\mathtt{a}) = 1, ..., C(\mathtt{z}) = 26.$$

to map characters to integers and to use the function

$$E : \{0, 1, 2, 3, ...26\} \to \{0, 1, 2, 3, ...26\} E(x) = ((7 \cdot x) + 5) \bmod 27$$

for encryption. The inverse of the function E is

$$E^{-1} : \{0, 1, 2, ..., 26\} \to \{0, 1, 2, ..., 26\} E^{-1}(x) = ((4 \cdot x) + 7) \bmod 27.$$

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:

$C(\mathtt{f}) =$___, $C(\mathtt{o}) =$___, $C(\mathtt{r}) =$___, $C(\mathtt{m}) =$___.

She encrypts these with the function E and gets

$E(C(\mathtt{f})) =$___, $E(C(\mathtt{o})) =$___, $E(C(\mathtt{r})) =$___, $E(C(\mathtt{m})) =$___.

Alice sends these integers to Bob.

Bob receives the message and evaluates the function E^{-1} at the integers send by Alice:

$E^{-1}(E(C(\mathtt{f}))) =$___, $E^{-1}(E(C(\mathtt{o}))) =$___, $E^{-1}(E(C(\mathtt{r}))) =$___, $E^{-1}(E(C(\mathtt{m}))) =$___.

An application of C^{-1} yields:

$C^{-1}(E^{-1}(E(C(\mathtt{f})))) =$ ___, $C^{-1}(E^{-1}(E(C(\mathtt{o})))) =$ ___, $C^{-1}(E^{-1}(E(C(\mathtt{r})))) =$ ___, $C^{-1}(E^{-1}(E(C(\mathtt{m})))) =$ ___

Bob has decrypted thesecret message:

____

Problem 8.4 (6) (1 point)

Bob receives an encrypted message from Alice:

`ogdcsjt`

First he applies the encoding function

$$C : \{-, \mathtt{a}, \mathtt{b}, \mathtt{c}, ..., \mathtt{z}\} \to \{0, 1, 2, 3, ...26\}, C(-) = 0, C(\mathtt{a}) = 1, ..., C(\mathtt{z}) = 26.$$

and obtains this sequence of integers:

____

Bob decrypts the message using the decryption function

$$D : \{0, 1, 2, 3, ...26\} \to \{0, 1, 2, 3, ...26\} D(x) = (14 \cdot (x - 4)) \bmod 27.$$

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:

$\mathtt{green} - \mathtt{alert}$

First she applies the encoding function

$$C : \{-, \mathtt{a}, \mathtt{b}, \mathtt{c}, ..., \mathtt{z}\} \rightarrow \{0, 1, 2, 3, ...26\}, C(-) = 0, C(\mathtt{a}) = 1, ..., C(\mathtt{z}) = 26.$$

and obtains this sequence of integers:

____

Then Alice encrypts the message using the encryption function

$$E : \{0, 1, 2, 3, \ldots, 26\} \rightarrow \{0, 1, 2, 3, \ldots, 26\}, E(x) = (4 \cdot x + 5) \bmod 27.$$

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

$$\mathbb{A} = \{-, \texttt{a}, \texttt{b}, \texttt{c}, ..., \texttt{z}\}$$

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 form Alice to Bob:

`kzrfygqyzyjmrymdydsl`

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 form Alice to Bob:

`oekqmzbbqieedqruczjqriqcktyqriqzqdvvuqwhecqoek`

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 $E : \mathbb{A} \to \mathbb{A}$ is given by:
$E(-) =$___,
$E(\texttt{a}) =$___,
$E(\texttt{b}) =$___,
$E(\texttt{c}) =$___,
$E(\texttt{d}) =$___,
$E(\texttt{e}) =$___,

$E(\mathtt{f}) =$___,
$E(\mathtt{g}) =$___,
$E(\mathtt{h}) =$___,
$E(\mathtt{i}) =$___,
$E(\mathtt{j}) =$___,
$E(\mathtt{k}) =$___,
$E(\mathtt{l}) =$___,
$E(\mathtt{m}) =$___,
$E(\mathtt{n}) =$___,
$E(\mathtt{o}) =$___,
$E(\mathtt{p}) =$___,
$E(\mathtt{q}) =$___,
$E(\mathtt{r}) =$___,
$E(\mathtt{s}) =$___,
$E(\mathtt{t}) =$___,
$E(\mathtt{u}) =$___,
$E(\mathtt{v}) =$___,
$E(\mathtt{w}) =$___,
$E(\mathtt{x}) =$___,
$E(\mathtt{y}) =$___,
$E(\mathtt{z}) =$___,

Now Eve also knows the **decryption** function $D : \mathbb{A} \to \mathbb{A}$. 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:

$D(-) =$___,
$D(\mathtt{a}) =$___,
$D(\mathtt{b}) =$___,
$D(\mathtt{c}) =$___,
$D(\mathtt{d}) =$___,
$D(\mathtt{e}) =$___,
$D(\mathtt{f}) =$___,
$D(\mathtt{g}) =$___,
$D(\mathtt{h}) =$___,
$D(\mathtt{i}) =$___,
$D(\mathtt{j}) =$___,
$D(\mathtt{k}) =$___,
$D(\mathtt{l}) =$___,
$D(\mathtt{m}) =$___,
$D(\mathtt{n}) =$___,
$D(\mathtt{o}) =$___,
$D(\mathtt{p}) =$___,
$D(\mathtt{q}) =$___,
$D(\mathtt{r}) =$___,
$D(\mathtt{s}) =$___,
$D(\mathtt{t}) =$___,

$D(\texttt{u}) =$___,
$D(\texttt{v}) =$___,
$D(\texttt{w}) =$___,
$D(\texttt{x}) =$___,
$D(\texttt{y}) =$___,
$D(\texttt{z}) =$___,

Using the function D Eve decrypts the message and obtains:

____

Problem 8.5 (4) (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 form Alice to Bob:

$$\texttt{xnawukqwoqnawsawzxjwikrawejwpeiawxj} - \texttt{wolxza}$$

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 $E : \mathbb{A} \to \mathbb{A}$ is given by:
$E(-) =$___,
$E(\texttt{a}) =$___,
$E(\texttt{b}) =$___,
$E(\texttt{c}) =$___,
$E(\texttt{d}) =$___,
$E(\texttt{e}) =$___,
$E(\texttt{f}) =$___,
$E(\texttt{g}) =$___,
$E(\texttt{h}) =$___,
$E(\texttt{i}) =$___,
$E(\texttt{j}) =$___,
$E(\texttt{k}) =$___,
$E(\texttt{l}) =$___,
$E(\texttt{m}) =$___,
$E(\texttt{n}) =$___,
$E(\texttt{o}) =$___,
$E(\texttt{p}) =$___,
$E(\texttt{q}) =$___,
$E(\texttt{r}) =$___,
$E(\texttt{s}) =$___,
$E(\texttt{t}) =$___,
$E(\texttt{u}) =$___,
$E(\texttt{v}) =$___,

$E(\mathtt{w}) =$___,
$E(\mathtt{x}) =$___,
$E(\mathtt{y}) =$___,
$E(\mathtt{z}) =$___,

Now Eve also knows the **decryption** function $D : \mathbb{A} \to \mathbb{A}$. 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:

$D(-) =$___,
$D(\mathtt{a}) =$___,
$D(\mathtt{b}) =$___,
$D(\mathtt{c}) =$___,
$D(\mathtt{d}) =$___,
$D(\mathtt{e}) =$___,
$D(\mathtt{f}) =$___,
$D(\mathtt{g}) =$___,
$D(\mathtt{h}) =$___,
$D(\mathtt{i}) =$___,
$D(\mathtt{j}) =$___,
$D(\mathtt{k}) =$___,
$D(\mathtt{l}) =$___,
$D(\mathtt{m}) =$___,
$D(\mathtt{n}) =$___,
$D(\mathtt{o}) =$___,
$D(\mathtt{p}) =$___,
$D(\mathtt{q}) =$___,
$D(\mathtt{r}) =$___,
$D(\mathtt{s}) =$___,
$D(\mathtt{t}) =$___,
$D(\mathtt{u}) =$___,
$D(\mathtt{v}) =$___,
$D(\mathtt{w}) =$___,
$D(\mathtt{x}) =$___,
$D(\mathtt{y}) =$___,
$D(\mathtt{z}) =$___,

Using the function D Eve decrypts the message and obtains:

____

Problem 8.5 (5) (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 form Alice to Bob:

zrqxeltxyzlrqxrmxykaxaltk

Eve counts the frequency of the characters and concludes that the character ___ has to be decrypted as the charater $-$ (space).

With this Eve finds the **decryption** function $D : \mathbb{A} \to \mathbb{A}$. 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:

$D(\texttt{-}) =$___,
$D(\texttt{a}) =$___,
$D(\texttt{b}) =$___,
$D(\texttt{c}) =$___,
$D(\texttt{d}) =$___,
$D(\texttt{e}) =$___,
$D(\texttt{f}) =$___,
$D(\texttt{g}) =$___,
$D(\texttt{h}) =$___,
$D(\texttt{i}) =$___,
$D(\texttt{j}) =$___,
$D(\texttt{k}) =$___,
$D(\texttt{l}) =$___,
$D(\texttt{m}) =$___,
$D(\texttt{n}) =$___,
$D(\texttt{o}) =$___,
$D(\texttt{p}) =$___,
$D(\texttt{q}) =$___,
$D(\texttt{r}) =$___,
$D(\texttt{s}) =$___,
$D(\texttt{t}) =$___,
$D(\texttt{u}) =$___,
$D(\texttt{v}) =$___,
$D(\texttt{w}) =$___,
$D(\texttt{x}) =$___,
$D(\texttt{y}) =$___,
$D(\texttt{z}) =$___,

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:

```
rdoqhvrbqseuoqckijqyrlvqvnjvdizedqzdqwekhquzhvtjzedi
```

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 $-$.

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:

```
tjpvywivhjq-vdivodh-
```

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 = _____ and
84411 mod 2821 = _____

-55426 div 2371 = _____ and
-55426 mod 2371 = _____

-91199 div 213 = _____ and
-91199 mod 213 = _____

-28711 div 2717 = _____ and
-28711 mod 2717 = _____

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 $\underline{\quad (A) \quad}$ if there exists $\underline{\quad (B) \quad}$ function $f : A \to B$.

(A): [select: | **cardinality** | **depth** | **height** | **volume** | **width**]

(B): [select: | **a good** | **an injective** | **an invertible** | **a nice** | **an onto**]

We say that the $\underline{\quad (C) \quad}$ of A is n if there is $\underline{\quad (D) \quad}$ function from A to $\underline{\quad (E) \quad}$.

(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** | $\{0,1,2,...,n-1\}$ | $\{0,1,2,...,n\}$ | $\{n\}$ | $\{-n,-n+1,-n+2,...,1\}$]

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 $f : \mathbb{Z}_3 \to \mathbb{Z}_3,\ f(x) = (2+x) \bmod 3$.

Evaluate f at all elements of the domain:

$f(0) =$ ___

$f(1) =$ ___

$f(2) =$ ___

The function f is invertible. Find the image of the inverse f^{-1} of f at all elements of its domain.

$f^{-1}(0) =$ ___

$f^{-1}(1) =$ ___

$f^{-1}(2) =$ ___

Problem 9.1 (3) (1 point)

Let D be a set. Assume there is an invertible function

$$h : D \to \mathbb{Z}_5$$

Then the cardinality of D is ___.

Problem 9.1 (4) (1 point)

Let X be a set. Assume there is an invertible function

$$g : X \to \{0, 1, 2, ..., 7\}.$$

Then the number of elements in X is ___.

Problem 9.1 (5) (1 point)

Let $X = \{-8, -7, -6, \ldots, 11\}$.

Because there is an invertible function

$h : \left\{0, 1, 2, ..., \_\_\_ \right\} \to X$

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. ___ $A = \{x \mid x \in \mathbb{N}$ and $x \bmod 2 = 0\}$ and $B = \mathbb{N}$
2. ___ $A = \{1, 2, 3, ..., 25\}$ and $B = \mathbb{Z}_{25}$
3. ___ $A = \{1, 2, 3, ..., 14\}$ and $B = \mathbb{Z}_{14}$
4. ___ $A = \{\ldots, -3, -2, -1\}$ and $B = \mathbb{N}$

Problem 9.1 (7) (1 point)

$\#\mathbb{Z}_{48}^{\otimes} =$ ______

Problem 9.1 (8) (1 point)

$\#\mathbb{Z}_{109} =$ ______

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 ______

Problem 9.1 (10) (1 point)

$\#\{\} =$ ______

Problem 9.1 (11) (1 point)

$\#\{\} =$ ___

$\#\{0\} =$ ___

$\#\{-30, -29, -28\} =$ ___

Problem 9.1 (12) (1 point)

The cardinality of the set $\{43, 44, 45, ..., 127\}$ is: ______

Solutions

Problem 9.1 (1) *Correct Answers:*

- cardinality
- an invertible
- cardinality
- an invertible
- `{0,1,2,...,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

9.2 Infinite Sets

Problem 9.2 (1) (1 point)

Complete the following:

Let A and B be nonempty sets.

We say that A and B have the same $\underline{\quad (A) \quad}$ if there exists $\underline{\quad (B) \quad}$ function $f : A \to B$.

(A): [select: | **cardinality** | **depth** | **height** | **volume** | **width**]

(B): [select: | **a good** | **an injective** | **an invertible** | **a nice** | **an onto**]

We say that A is $\underline{\quad (C) \quad}$ if for some $n \in \mathbb{N}$ there is $\underline{\quad (D) \quad}$ function from A to $\underline{\quad (E) \quad}$.

(C): [select: | **finite** | **infinite** | **good** | **bad** | **nice** | **boring**]

(D): [select: | **a good** | **an injective** | **an invertible** | **a nice** | **an onto**]

(E): [select: | **the set of natural numbers** | **the set of integers** | $\{0, 1, 2, ..., n-1\}$]

If no such function exists we call A ________.

[select: | **finite** | **infinite** | **good** | **bad** | **nice** | **boring**]

Problem 9.2 (2) (1 point)

Special Sets

Match the two representation of sets. Enter the letters next to the numbers.

___ 1. $\mathbb{Z}_{21}$	A. $\{0, 1, 2, 3, \ldots, 20\}$
___ 2. $\mathbb{Z}_{21}^{\otimes}$	B. $\{1, 2, 3, \ldots, 20\}$
___ 3. $\mathbb{Z}_{16}$	C. $\{0, 1, 2, 3, \ldots, 15\}$

Problem 9.2 (3) (1 point)

Determine whether the two sets have the same cardinality.

1. ___ $\{1,2,3,\ldots,2324\}$ 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 $\underline{\quad(A)\quad}$ if there exists $\underline{\quad(B)\quad}$ function $f : A \to B$.

(A): [select: | **cardinality** | **depth** | **height** | **volume** | **width**]

(B): [select: | **a good** | **an injective** | **an invertible** | **a nice** | **an onto**]

We say that A is $\underline{\quad(C)\quad}$ if there is $\underline{\quad(D)\quad}$ 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. ___ $\{-7,-6,-5,...,1\}$
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. ___ $\{-15, -14, -13, ..., 7\}$
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,...,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.

$A \times B = \{$ ______________________ $\}$

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 $A = \{1,2,3,...,6\}$ and $B = \{1,2,3,...,10\}$.

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 $A = \{4, 5, 6, ..., 15\}$ and $B = \{4, 5, 6, ..., 18\}$.

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.

$A \times B = \{$_________$\}$

[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, $A \times B = \{(a,b) | a \in A \textbf{ and } b \in B\}$

Thus, $A \times B$ is
$\{(a,1),(a,2),(a,3),(b,1),(b,2),(b,3),(c,1),(c,2),(c,3)\}$

- 9
- $(\mathrm{a},1),(\mathrm{a},2),(\mathrm{a},3),(\mathrm{b},1),(\mathrm{b},2),(\mathrm{b},3),(\mathrm{c},1),(\mathrm{c},2),(\mathrm{c},3)$

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 $A = \{a_1, a_2, a_3, \ldots, a_n\}$.

Let N be the number of distinct subsets of A.

Let b be an element not contained in A.

Let $B = \{a_1, a_2, a_3, \ldots, a_n, b\}$, 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 $S = \{6,7,8,...,15\}$.

The cardinality of S is: ___

Thus the number of distinct subsets of $\{6,7,8,...,15\}$ is: ___

Problem 9.4 (5) (1 point)

The number of distinct subsets of 6,7,8,...,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 mod 13= ___,
we have that 13 ___ 52.   [select: | **divides** | **does not divide**]

Because 42 mod 18= ___,
we have that 18 ___ 42.   [select: | **divides** | **does not divide**]

Because 8 mod 18= ___,
we have that 18 ___ 8.   [select: | **divides** | **does not divide**]

Because 6 mod 20= ___,
we have that 20 ___ 6.   [select: | **divides** | **does not divide**]

Because 6 mod 3= ___,
we have that 3 ___ 6.   [select: | **divides** | **does not divide**]

Because 25 mod 20= ___,
we have that 20 ___ 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:

$(a+a) \bmod 3 =$ ___

$(a+b) \bmod 3 =$ ___

$(a \cdot b) \bmod 3 =$ ___

$(a+2) \bmod 3 =$ ___

$(2 \cdot b) \bmod 3 =$ ___

Solutions

Problem 10.2 (1) *Correct Answers:*

- ACDEFGIJKMOPQSUVWY

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
$\gcd(a,b) =$ _________

Problem 10.3 (5) **(1 point)**

Compute the remainder and complete the statement about divisibility

Because 69 mod 16= ___,
we have that 16 ___ 69. [select: | **divides** | **does not divide**]

Because 44 mod 11= ___,
we have that 11 ___ 44. [select: | **divides** | **does not divide**]

Because 5 mod 20= ___,
we have that 20 ___ 5. [select: | **divides** | **does not divide**]

Because 102 mod 17= ___,
we have that 17 ___ 102. [select: | **divides** | **does not divide**]

Because 75 mod 6= ___,
we have that 6 ___ 75. [select: | **divides** | **does not divide**]

Because 2 mod 7= ___,
we have that 7 ___ 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=___ (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 $\underline{\quad(A)\quad}$ and $\underline{\quad(B)\quad}$.

(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 $\underline{\quad (A) \quad}$ and $\underline{\quad (B) \quad}$.

(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 $\underline{\quad (A) \quad}$ and $\underline{\quad (B) \quad}$.

(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 $\underline{\quad (A) \quad}$ and $\underline{\quad (B) \quad}$.

(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 $\underline{\quad (A) \quad}$ and $\underline{\quad (B) \quad}$.

(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 $\underline{\quad (A) \quad}$ and $\underline{\quad (B) \quad}$.

(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 $\underline{\quad (A) \quad}$ and $\underline{\quad (B) \quad}$.

(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 $\underline{\quad (A) \quad}$ and $\underline{\quad (B) \quad}$.

(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 $\underline{\quad (A) \quad}$ and $\underline{\quad (B) \quad}$.

(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 $\underline{\quad (A) \quad}$ and $\underline{\quad (B) \quad}$.

(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 $\underline{\quad (A) \quad}$ and $\underline{\quad (B) \quad}$.

(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=___ (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 $\underline{\quad (A) \quad}$ and $\underline{\quad (B) \quad}$.

(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 $\underline{\quad (A) \quad}$ and $\underline{\quad (B) \quad}$.

(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 $\underline{\quad (A) \quad}$ and $\underline{\quad (B) \quad}$.

(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 $\underline{\quad (A) \quad}$ and $\underline{\quad (B) \quad}$.

(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 $\underline{\quad (A) \quad}$ and $\underline{\quad (B) \quad}$.

(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 $\underline{\quad (A) \quad}$ and $\underline{\quad (B) \quad}$.

(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 $\underline{\quad (A) \quad}$ and $\underline{\quad (B) \quad}$.

(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 $\underline{\quad (A) \quad}$ and $\underline{\quad (B) \quad}$.

(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 $\underline{\quad (A) \quad}$ and $\underline{\quad (B) \quad}$.

(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 $\underline{\quad (A) \quad}$ and $\underline{\quad (B) \quad}$.

(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 $\underline{\quad (A) \quad}$ and $\underline{\quad (B) \quad}$.

(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 $p_1, p_2, ..., p_n$ and let $q = p_1 \cdot p_2 \cdot \cdots \cdot p_n$. [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 $\underline{\quad (A) \quad}$ $q+1$ but $\underline{\quad (B) \quad}$ 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 $\mathbb{Z}_n^{\otimes} := \{1, 2, 3, \ldots, n-1\}$.
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 $\underline{\ \ (A)\ \ }$ and is $\underline{\ \ (B)\ \ }$.

(A): [select: | **prime** | **not prime**]

(B): [select: | **in a twin prime pair** | **not in a twin prime pair**]

21 is $\underline{\quad (A) \quad}$ and is $\underline{\quad (B) \quad}$.

(A): [select: | **prime** | **not prime**]

(B): [select: | **in a twin prime pair** | **not in a twin prime pair**]

39 is $\underline{\quad (A) \quad}$ and is $\underline{\quad (B) \quad}$.

(A): [select: | **prime** | **not prime**]

(B): [select: | **in a twin prime pair** | **not in a twin prime pair**]

47 is $\underline{\quad (A) \quad}$ and is $\underline{\quad (B) \quad}$.

(A): [select: | **prime** | **not prime**]

(B): [select: | **in a twin prime pair** | **not in a twin prime pair**]

63 is $\underline{\quad (A) \quad}$ and is $\underline{\quad (B) \quad}$.

(A): [select: | **prime** | **not prime**]

(B): [select: | **in a twin prime pair** | **not in a twin prime pair**]

77 is $\underline{\quad (A) \quad}$ and is $\underline{\quad (B) \quad}$.

(A): [select: | **prime** | **not prime**]

(B): [select: | **in a twin prime pair** | **not in a twin prime pair**]

83 is $\underline{\quad (A) \quad}$ and is $\underline{\quad (B) \quad}$.

(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.

$\_\_\_ \cdot 10^6 + \_\_\_ \cdot 10^5 + \_\_\_ \cdot 10^4 + \_\_\_ \cdot 10^3 + \_\_\_ \cdot 10^2 + \_\_\_ \cdot 10 + \_\_\_ \cdot 1$

Problem 11.1 (2) (1 point)

Give the expanded decimal form of 90884.

$\_\_\_ \cdot 10^6 + \_\_\_ \cdot 10^5 + \_\_\_ \cdot 10^4 + \_\_\_ \cdot 10^3 + \_\_\_ \cdot 10^2 + \_\_\_ \cdot 10 + \_\_\_ \cdot 1$

Problem 11.1 (3) (1 point)

What are the place values of a base 10 number with 5 digits?

leftmost digit $\rightarrow$ ___ ___ ___ ___ ___ $\leftarrow$ rightmost digit

---

Problem 11.1 (4) (1 point)

Compute:

20838260094400860294 mod 10 = ____

20838260094400860294 mod 100 = ____

20838260094400860294 mod 1000 = ____

20838260094400860294 mod 10000 = ____

20838260094400860294 mod 100000 = ____

20838260094400860294 mod 1000000 = ____

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.

$\_\_\_ \cdot 2^6 + \_\_\_ \cdot 2^5 + \_\_\_ \cdot 2^4 + \_\_\_ \cdot 2^3 + \_\_\_ \cdot 2^2 + \_\_\_ \cdot 2 + \_\_\_ \cdot 1$

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 $\rightarrow$ ___ ___ ___ ___ ___ $\leftarrow$ rightmost digit

Convert these base 2 numbers to decimal numbers.

$0_2 =$___ $1_2 =$___

$10_2 =$___ $11_2 =$___

$100_2 =$___ $101_2 =$___ $110_2 =$___

$1000_2 =$___ $1001_2 =$___ $1010_2 =$___ $1110_2 =$___

Problem 11.2 (3) **(1 point)**

Give the expanded base 2 form of 101110_2.

$\_\_\_ \cdot 2^6 + \_\_\_ \cdot 2^5 + \_\_\_ \cdot 2^4 + \_\_\_ \cdot 2^3 + \_\_\_ \cdot 2^2 + \_\_\_ \cdot 2 + \_\_\_ \cdot 1$

Give 101110_2 in decimal representation.

____

Problem 11.2 (4) **(1 point)**

Give the expanded base 2 form of 111101_2.

$\_\_\_ \cdot 2^6 + \_\_\_ \cdot 2^5 + \_\_\_ \cdot 2^4 + \_\_\_ \cdot 2^3 + \_\_\_ \cdot 2^2 + \_\_\_ \cdot 2 + \_\_\_ \cdot 1$

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.

$\_\_\_\__2 = \_\_\_ \cdot 2^4 + \_\_\_ \cdot 2^3 + \_\_\_ \cdot 2^2 + \_\_\_ \cdot 2^1 + \_\_\_ \cdot 2^0 = 0$

$\_\_\_\__2 = \_\_\_ \cdot 2^4 + \_\_\_ \cdot 2^3 + \_\_\_ \cdot 2^2 + \_\_\_ \cdot 2^1 + \_\_\_ \cdot 2^0 = 1$

$\_\_\_\__2 = \_\_\_ \cdot 2^4 + \_\_\_ \cdot 2^3 + \_\_\_ \cdot 2^2 + \_\_\_ \cdot 2^1 + \_\_\_ \cdot 2^0 = 2$

$\_\_\_\__2 = \_\_\_ \cdot 2^4 + \_\_\_ \cdot 2^3 + \_\_\_ \cdot 2^2 + \_\_\_ \cdot 2^1 + \_\_\_ \cdot 2^0 = 3$

$\_\_\_\__2 = \_\_\_ \cdot 2^4 + \_\_\_ \cdot 2^3 + \_\_\_ \cdot 2^2 + \_\_\_ \cdot 2^1 + \_\_\_ \cdot 2^0 = 4$

$\_\_\_\__2 = \_\_\_ \cdot 2^4 + \_\_\_ \cdot 2^3 + \_\_\_ \cdot 2^2 + \_\_\_ \cdot 2^1 + \_\_\_ \cdot 2^0 = 5$

$\_\_\_\__2 = \_\_\_ \cdot 2^4 + \_\_\_ \cdot 2^3 + \_\_\_ \cdot 2^2 + \_\_\_ \cdot 2^1 + \_\_\_ \cdot 2^0 = 6$

$\_\_\_\__2 = \_\_\_ \cdot 2^4 + \_\_\_ \cdot 2^3 + \_\_\_ \cdot 2^2 + \_\_\_ \cdot 2^1 + \_\_\_ \cdot 2^0 = 7$

$\_\_\_\__2 = \_\_\_ \cdot 2^4 + \_\_\_ \cdot 2^3 + \_\_\_ \cdot 2^2 + \_\_\_ \cdot 2^1 + \_\_\_ \cdot 2^0 = 8$

$\_\_\_\__2 = \_\_\_ \cdot 2^4 + \_\_\_ \cdot 2^3 + \_\_\_ \cdot 2^2 + \_\_\_ \cdot 2^1 + \_\_\_ \cdot 2^0 = 9$

$\_\_\_\__2 = \_\_\_ \cdot 2^4 + \_\_\_ \cdot 2^3 + \_\_\_ \cdot 2^2 + \_\_\_ \cdot 2^1 + \_\_\_ \cdot 2^0 = 10$

$\_\_\_\__2 = \_\_\_ \cdot 2^4 + \_\_\_ \cdot 2^3 + \_\_\_ \cdot 2^2 + \_\_\_ \cdot 2^1 + \_\_\_ \cdot 2^0 = 11$

$\_\_\_\__2 = \_\_\_ \cdot 2^4 + \_\_\_ \cdot 2^3 + \_\_\_ \cdot 2^2 + \_\_\_ \cdot 2^1 + \_\_\_ \cdot 2^0 = 12$

$\_\_\_\__2 = \_\_\_ \cdot 2^4 + \_\_\_ \cdot 2^3 + \_\_\_ \cdot 2^2 + \_\_\_ \cdot 2^1 + \_\_\_ \cdot 2^0 = 13$

$\_\_\_\__2 = \_\_\_ \cdot 2^4 + \_\_\_ \cdot 2^3 + \_\_\_ \cdot 2^2 + \_\_\_ \cdot 2^1 + \_\_\_ \cdot 2^0 = 14$

$\_\_\_\__2 = \_\_\_ \cdot 2^4 + \_\_\_ \cdot 2^3 + \_\_\_ \cdot 2^2 + \_\_\_ \cdot 2^1 + \_\_\_ \cdot 2^0 = 15$

$\_\_\_\__2 = \_\_\_ \cdot 2^4 + \_\_\_ \cdot 2^3 + \_\_\_ \cdot 2^2 + \_\_\_ \cdot 2^1 + \_\_\_ \cdot 2^0 = 16$

$\_\_\_\__2 = \_\_\_ \cdot 2^4 + \_\_\_ \cdot 2^3 + \_\_\_ \cdot 2^2 + \_\_\_ \cdot 2^1 + \_\_\_ \cdot 2^0 = 17$

$\underline{\quad\quad}_2 = \underline{\quad}\cdot 2^4 + \underline{\quad}\cdot 2^3 + \underline{\quad}\cdot 2^2 + \underline{\quad}\cdot 2^1 + \underline{\quad}\cdot 2^0 = 18$

$\underline{\quad\quad}_2 = \underline{\quad}\cdot 2^4 + \underline{\quad}\cdot 2^3 + \underline{\quad}\cdot 2^2 + \underline{\quad}\cdot 2^1 + \underline{\quad}\cdot 2^0 = 19$

Problem 11.2 (6) (1 point)

Convert these integers from binary to decimal representation:

$1_2 =$ ______________

$10_2 =$ ______________

$111_2 =$ ______________

$1110_2 =$ ______________

$10000_2 =$ ______________

$100110_2 =$ ______________

$1010011_2 =$ ______________

$11010100_2 =$ ______________

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 $a :=$ ___

Let $q_0 := a$.

Let $r_0 := q_0 \bmod 2 =$ ___. Let $q_1 := q_0 \operatorname{div} 2 =$ _____.

Let $r_1 := q_1 \bmod 2 =$ ___. Let $q_2 := q_1 \operatorname{div} 2 =$ _____.

Let $r_2 := q_2 \bmod 2 =$ ___. Let $q_3 := q_2 \operatorname{div} 2 =$ _____.

Let $r_3 := q_3 \bmod 2 =$ ___. Let $q_4 := q_3 \operatorname{div} 2 =$ _____.

Output: The expanded base 2 representation of the decimal number 15 is:

$15 = r_3 \cdot 2^3$
$+r_2 \cdot 2^2$
$+r_1 \cdot 2^1$
$+r_0 \cdot 2^0$

$=$ ___ $\cdot 2^3$
$+$ ___ $\cdot 2^2$
$+$ ___ $\cdot 2^1$
$+$ ___ $\cdot 2^0$

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.]

$15 =$ _____$_2$

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 $a :=$ ___

Let $q_0 := a$.

Let $r_0 := q_0 \bmod 2 =$ ___. Let $q_1 := q_0 \operatorname{div} 2 =$ _____.

Let $r_1 := q_1 \bmod 2 =$ ___. Let $q_2 := q_1 \operatorname{div} 2 =$ _____.

Let $r_2 := q_2 \bmod 2 =$ ___. Let $q_3 := q_2 \operatorname{div} 2 =$ _____.

Let $r_3 := q_3 \bmod 2 =$ ___. Let $q_4 := q_3 \operatorname{div} 2 =$ _____.

Output: The expanded base 2 representation of the decimal number 11 is:

$11 = r_3 \cdot 2^3$
$+r_2 \cdot 2^2$
$+r_1 \cdot 2^1$
$+r_0 \cdot 2^0$

$=$ ___ $\cdot 2^3$
$+$ ___ $\cdot 2^2$
$+$ ___ $\cdot 2^1$
$+$ ___ $\cdot 2^0$

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.]

$11 =$ _____$_2$

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.]

$31 =$ _________$_2$

$93 =$ _________$_2$

$168 =$ _________$_2$

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.]

$46 = \underline{\hspace{2cm}}_2$

$92 = \underline{\hspace{2cm}}_2$

$339 = \underline{\hspace{2cm}}_2$

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.

$\_\_\_ \cdot 6^6 + \_\_\_ \cdot 6^5 + \_\_\_ \cdot 6^4 + \_\_\_ \cdot 6^3 + \_\_\_ \cdot 6^2 + \_\_\_ \cdot 6 + \_\_\_ \cdot 1$

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.

$\_\_\_ \cdot 12^6 + \_\_\_ \cdot 12^5 + \_\_\_ \cdot 12^4 + \_\_\_ \cdot 12^3 + \_\_\_ \cdot 12^2 + \_\_\_ \cdot 12 + \_\_\_ \cdot 1$

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.

$\_\_\_ \cdot 6^6 + \_\_\_ \cdot 6^5 + \_\_\_ \cdot 6^4 + \_\_\_ \cdot 6^3 + \_\_\_ \cdot 6^2 + \_\_\_ \cdot 6 + \_\_\_ \cdot 1$

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.

$\_\_\_ \cdot 18^6 + \_\_\_ \cdot 18^5 + \_\_\_ \cdot 18^4 + \_\_\_ \cdot 18^3 + \_\_\_ \cdot 18^2 + \_\_\_ \cdot 18 + \_\_\_ \cdot 1$

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.

$0_6 =$___ $1_6 =$___ $3_6 =$___ $5_6 =$___

$10_6 =$___ $11_6 =$___ $50_6 =$___ $42_6 =$___

$100_6 =$___ $101_6 =$___ $110_6 =$___ $533_6 =$___

$1000_6 =$___ $1005_6 =$___ $1030_6 =$___ $5330_6 =$___

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.

$0_{16} =$___ $1_{16} =$___ $7_{16} =$___ $F_{16} =$___

$10_{16} =$___ $11_{16} =$___ $D7_{16} =$___ $37_{16} =$___

$100_{16} =$___ $101_{16} =$___ $110_{16} =$___ $813_{16} =$___

$1000_{16} =$___ $100F_{16} =$___ $1070_{16} =$___ $8130_{16} =$___

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.

$\_\_\_\__5 =$
$\_\_\_ \cdot 5^1 +$

$\_\_\_ \cdot 5^0 = 0$

$\_\_\_\__5 =$
$\_\_\_ \cdot 5^1 +$
$\_\_\_ \cdot 5^0 = 1$

$\_\_\_\__5 =$
$\_\_\_ \cdot 5^1 +$
$\_\_\_ \cdot 5^0 = 2$

$\_\_\_\__5 =$
$\_\_\_ \cdot 5^1 +$
$\_\_\_ \cdot 5^0 = 3$

$\_\_\_\__5 =$
$\_\_\_ \cdot 5^1 +$
$\_\_\_ \cdot 5^0 = 4$

$\_\_\_\__5 =$
$\_\_\_ \cdot 5^1 +$
$\_\_\_ \cdot 5^0 = 5$

$\_\_\_\__5 =$
$\_\_\_ \cdot 5^1 +$
$\_\_\_ \cdot 5^0 = 6$

$\_\_\_\__5 =$
$\_\_\_ \cdot 5^1 +$
$\_\_\_ \cdot 5^0 = 7$

$\_\_\_\__5 =$
$\_\_\_ \cdot 5^1 +$
$\_\_\_ \cdot 5^0 = 8$

$\_\_\_\__5 =$
$\_\_\_ \cdot 5^1 +$
$\_\_\_ \cdot 5^0 = 9$

$\_\_\_\__5 =$
$\_\_\_ \cdot 5^1 +$
$\_\_\_ \cdot 5^0 = 10$

$\_\_\_\__5 =$
$\_\_\_ \cdot 5^1 +$
$\_\_\_ \cdot 5^0 = 11$

$\_\_\_\__5 =$

$\underline{\quad}\cdot 5^1 +$
$\underline{\quad}\cdot 5^0 = 12$

$\underline{\qquad}_5 =$
$\underline{\quad}\cdot 5^1 +$
$\underline{\quad}\cdot 5^0 = 13$

$\underline{\qquad}_5 =$
$\underline{\quad}\cdot 5^1 +$
$\underline{\quad}\cdot 5^0 = 14$

$\underline{\qquad}_5 =$
$\underline{\quad}\cdot 5^1 +$
$\underline{\quad}\cdot 5^0 = 15$

$\underline{\qquad}_5 =$
$\underline{\quad}\cdot 5^1 +$
$\underline{\quad}\cdot 5^0 = 16$

$\underline{\qquad}_5 =$
$\underline{\quad}\cdot 5^1 +$
$\underline{\quad}\cdot 5^0 = 17$

$\underline{\qquad}_5 =$
$\underline{\quad}\cdot 5^1 +$
$\underline{\quad}\cdot 5^0 = 18$

$\underline{\qquad}_5 =$
$\underline{\quad}\cdot 5^1 +$
$\underline{\quad}\cdot 5^0 = 19$

$\underline{\qquad}_5 =$
$\underline{\quad}\cdot 5^1 +$
$\underline{\quad}\cdot 5^0 = 20$

$\underline{\qquad}_5 =$
$\underline{\quad}\cdot 5^1 +$
$\underline{\quad}\cdot 5^0 = 21$

$\underline{\qquad}_5 =$
$\underline{\quad}\cdot 5^1 +$
$\underline{\quad}\cdot 5^0 = 22$

$\underline{\qquad}_5 =$
$\underline{\quad}\cdot 5^1 +$
$\underline{\quad}\cdot 5^0 = 23$

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 $b :=$ ___ and a base 10 number $a :=$ ___

Let $q_0 := a$.

Let $r_0 := q_0 \bmod b =$ ___. Let $q_1 := a_0 \operatorname{div} b =$ _____.

Let $r_1 := q_1 \bmod b =$ ___. Let $q_2 := a_1 \operatorname{div} b =$ _____.

Let $r_2 := q_2 \bmod b =$ ___. Let $q_3 := a_2 \operatorname{div} b =$ _____.

Let $r_3 := q_3 \bmod b =$ ___. Let $q_4 := a_3 \operatorname{div} b =$ _____.

Let $r_4 := q_4 \bmod b =$ ___. Let $q_5 := a_4 \operatorname{div} b =$ _____.

Let $r_5 := q_5 \bmod b =$ ___. Let $q_6 := a_5 \operatorname{div} b =$ _____.

Output: The expanded base 7 representation of the decimal number 66073 is:

$66073 = r_5 \cdot 7^5 + r_4 \cdot 7^4 + r_3 \cdot 7^3 + r_2 \cdot 7^2 + r_1 \cdot 7^1 + r_0 \cdot 7^0$

$= \_\_\_ \cdot 7^5 + \_\_\_ \cdot 7^4 + \_\_\_ \cdot 7^3 + \_\_\_ \cdot 7^2 + \_\_\_ \cdot 7^1 + \_\_\_ \cdot 7^0$

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.]

$66073 = \_\_\_\_\__7$

Problem 11.5 (2) (1 point)

With the conversion algorithm find the base 13 representation of the decimal number 27322.

Input: Base $b :=$ ___ and a base 10 number $a :=$ ___

Let $q_0 := a$.

Let $r_0 := q_0 \bmod b =$ ___. Let $q_1 := a_0 \operatorname{div} b =$ _____.

Let $r_1 := q_1 \bmod b =$ ___. Let $q_2 := a_1 \operatorname{div} b =$ _____.

Let $r_2 := q_2 \bmod b =$ ___. Let $q_3 := a_2 \operatorname{div} b =$ _____.

Let $r_3 := q_3 \bmod b =$ ___. Let $q_4 := a_3 \operatorname{div} b =$ _____.

Output: The expanded base 13 representation of the decimal number 27322 is:

$27322 = r_3 \cdot 13^3 + r_2 \cdot 13^2 + r_1 \cdot 13^1 + r_0 \cdot 13^0$

$= \_\_\_ \cdot 13^3 + \_\_\_ \cdot 13^2 + \_\_\_ \cdot 13^1 + \_\_\_ \cdot 13^0$

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.]

$27322 = \_\_\_\_\__{13}$

Problem 11.5 (3) (1 point)

With the conversion algorithm find the base 17 representation of the decimal number 50391.

Input: Base $b :=$ ___ and a base 10 number $a :=$ ___

Let $q_0 := a$.

Let $r_0 := q_0 \bmod b =$ ___. Let $q_1 := a_0 \operatorname{div} b =$ _____.

Let $r_1 := q_1 \bmod b =$ ___. Let $q_2 := a_1 \operatorname{div} b =$ _____.

Let $r_2 := q_2 \bmod b =$ ___. Let $q_3 := a_2 \operatorname{div} b =$ _____.

Let $r_3 := q_3 \bmod b =$ ___. Let $q_4 := a_3 \operatorname{div} b =$ _____.

Output: The expanded base 17 representation of the decimal number 50391 is:

$50391 = r_3 \cdot 17^3 + r_2 \cdot 17^2 + r_1 \cdot 17^1 + r_0 \cdot 17^0$

$= \_\_\_ \cdot 17^3 + \_\_\_ \cdot 17^2 + \_\_\_ \cdot 17^1 + \_\_\_ \cdot 17^0$

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.]

$50391 = \_\_\_\_\__{17}$

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.]

$1 = \_\_\_\_\__{6}$ $2 = \_\_\_\_\__{6}$

$6 = \_\_\_\_\__{6}$ $6 = \_\_\_\_\__{6}$

$36 = \_\_\_\_\__{6}$ $36 = \_\_\_\_\__{6}$

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.]

$1 = \_\_\_\_\__{13}$ $10 = \_\_\_\_\__{13}$

$13 = \_\_\_\_\__{13}$ $13 = \_\_\_\_\__{13}$

$169 = \_\_\_\_\__{13}$ $2028 = \_\_\_\_\__{13}$

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.]

$1 = \_\_\_\_\__{17}$ $1 = \_\_\_\_\__{17}$

$17 = \_\_\_\_\__{17}$ $119 = \_\_\_\_\__{17}$

$289 = \_\_\_\_\__{17}$ $3757 = \_\_\_\_\__{17}$

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.]

$1472 = \_\_\_\__5$

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.]

$9984788 = \_\_\_\_\_\__{15}$

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.

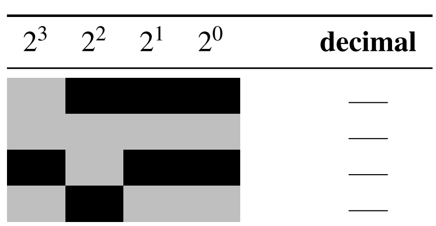
Black is represented by 1. The pixel on the left is represented by the most significant binary digit.

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.



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 ?

- A.
  ■■□□□
  □□■■□
  □□□□■

- B.
  □■■■□
  ■■□■□
  ■■□■□

- C.
  ■■■■□
  □■■■■
  ■■□■□

- D.
  □■■■■
  ■■□■■
  ■□□■□

- E.
  ■■■□□
  ■■□■■
  ■■□■■

- F.
  ■■■■□
  □■■■□
  ■■□■□

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.

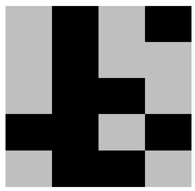
3
4
4
4
3

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

$2^4 \quad 2^3 \quad 2^2 \quad 2^1 \quad 2^0$

$$10010_2 = 1{\cdot}2^4 + 0{\cdot}2^3 + 0{\cdot}2^2 + 1{\cdot}2^1 + 0{\cdot}2^0 = 18$$
$$01011_2 = 0{\cdot}2^4 + 1{\cdot}2^3 + 0{\cdot}2^2 + 1{\cdot}2^1 + 1{\cdot}2^0 = 11$$

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

$2^4 \quad 2^3 \quad 2^2 \quad 2^1 \quad 2^0$

$10010_2 = 1{\cdot}2^4 + 0{\cdot}2^3 + 0{\cdot}2^2 + 1{\cdot}2^1 + 0{\cdot}2^0 = 18$

$01011_2 = 0{\cdot}2^4 + 1{\cdot}2^3 + 0{\cdot}2^2 + 1{\cdot}2^1 + 1{\cdot}2^0 = 11$

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:*

- FFFFFF
- 00FF00
- 0000FF
- FF0000

Problem 12.2 (7) *Correct Answers:*

- 0000FF
- 000000
- FFFFFF
- 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

12.3 Text

Problem 12.3 (1) (1 point)

A word is encoded in the integer:

4560413

We find the digits of the base 27 representation

$4560413 = \_\_\_ \cdot 27^4 + \_\_\_ \cdot 27^3 + \_\_\_ \cdot 27^2 + \_\_\_ \cdot 27 + \_\_\_$

Applying the inverse

$C^{-1} : \{0,1,2,3,\ldots,26\} \to \{-,\mathtt{a},\mathtt{b},\mathtt{c},\ldots,\mathtt{z}\}$ with $C^{-1}(0) = -$, $C^{-1}(1) = \mathtt{a}$, $C^{-1}(2) = \mathtt{b}$, …, $C^{-1}(26) = \mathtt{z}$,

of the encoding function C to these integers we obtain the word:

____

Problem 12.3 (2) (1 point)

We want to compute a representation of the word

`star`

by one integer in decimal representation.

First represent the characters in the word by integers using the encoding function

$C : \{-,\mathtt{a},\mathtt{b},\ldots,\mathtt{z}\} \to \{0,1,2,3,...26\}$ with $C(-) = 0$, $C(\mathtt{a}) = 1$,...,$C(\mathtt{z}) = 26$.

We obtain

$C(\mathtt{s}) = \_\_\_$, $C(\mathtt{t}) = \_\_\_$, $C(\mathtt{a}) = \_\_\_$, $C(\mathtt{r}) = \_\_\_$.

Then we compute the representation as one integer:

$C(\mathtt{s}) \cdot 27^3 + C(\mathtt{t}) \cdot 27^2 + C(\mathtt{a}) \cdot 27 + C(\mathtt{r}) = \_\_\_\_$

Problem 12.3 (3) (1 point)

Words can be encoded in the integer by applying the encoding function C:

$C : \{-,\mathtt{a},\mathtt{b},\ldots,\mathtt{z}\} \to \{0,1,2,3,...26\}$ with $C(-) = 0$, $C(\mathtt{a}) = 1$,...,$C(\mathtt{z}) = 26$.

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 `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,

$C : \{-, \mathtt{a}, \mathtt{b}, \ldots, \mathtt{z}\} \to \{0, 1, 2, 3, ...26\}$ with $C(-) = 0$, $C(\mathtt{a}) = 1$,...,$C(\mathtt{z}) = 26$.

(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:

$C : \{-, \mathtt{a}, \mathtt{b}, \ldots, \mathtt{z}\} \to \{0, 1, 2, 3, ...26\}$ with $C(-) = 0$, $C(\mathtt{a}) = 1$,...,$C(\mathtt{z}) = 26$.

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,

$C : \{-, \mathtt{a}, \mathtt{b}, \ldots, \mathtt{z}\} \to \{0, 1, 2, 3, ...26\}$ with $C(-) = 0$, $C(\mathtt{a}) = 1$,...,$C(\mathtt{z}) = 26$.

(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

$$C(\mathtt{h}) \cdot 27^4 + C(\mathtt{a}) \cdot 27^3 + C(\mathtt{r}) \cdot 27^2 + C(\mathtt{e}) \cdot 27 + C(\mathtt{s}).$$

Correct Answers:

- 4284487

Problem 12.3 (4) *Correct Answers:*

- mouse

Problem 12.3 (5) *Correct Answers:*

Hint: We encode `worms` as

$$C(\mathtt{w}) \cdot 27^4 + C(\mathtt{o}) \cdot 27^3 + C(\mathtt{r}) \cdot 27^2 + C(\mathtt{m}) \cdot 27 + C(\mathtt{s}).$$

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 = ___
g $\star$ f = ___

e $\star$ d = ___
d $\star$ e = ___

(e $\star$ d) $\star$ e = ___
e $\star$ (d $\star$ e) = ___

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

$$(a,b) \oplus (c,d) = \big((a+c) \bmod 2, (b+d) \bmod 2\big).$$

$\oplus$	**(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 = ___
j $\star$ g = ___

e $\star$ h = ___
h $\star$ k = ___

(e $\star$ h) $\star$ k = ___
e $\star$ (h $\star$ k) = ___

Problem 13.1 (5) **(1 point)**

Fill in the operation table for the binary operation $\otimes$ on the set $\mathbb{Z}_3$ defined by $a \otimes b = (a \cdot b)$ mod 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 × S → S be a binary operation on S. We read a * b as 'a star b'.

If ___(A)___ = (a * b) * c ___(B)___, then the binary operation * is called ___(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 $\ominus : \mathbb{Z}_{14} \times \mathbb{Z}_{14} \to \mathbb{Z}_{14}$ given by $a \ominus b = (a-b)$ mod 14.
2. ___ The operation $\star : \mathbb{Z}_{16}^{\otimes} \times \mathbb{Z}_{16}^{\otimes} \to \mathbb{Z}_{16}^{\otimes}$ given by $a \star b = (a^b)$ mod 16.
3. ___ The operation subtraction $- : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$.

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 mod $5 = 2$ and b mod $5 = 3$.

Find:

$(a+a)$ mod 5 = ___

$(a+b)$ mod 5 = ___

$(a \cdot b)$ mod 5 = ___

$(a+4)$ mod 5 = ___

$(4 \cdot b)$ mod 5 = ___

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 $\to$ 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 $\underline{\quad (A) \quad}$ for $\underline{\quad (B) \quad}$.

(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 $\ominus : \mathbb{Z}_4 \times \mathbb{Z}_4 \to \mathbb{Z}_4$ 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 $\oplus : \mathbb{Z}_8 \times \mathbb{Z}_8 \to \mathbb{Z}_8$ 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 $\otimes : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ 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 × S → 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]

Determine for which of these operations there is an identity in the corresponding set.

1. ___ The operation $\ominus : \mathbb{Z}_3 \times \mathbb{Z}_3 \to \mathbb{Z}_3$ given by $a \ominus b = (a-b) \bmod 3$.
2. ___ The operation $\star : \mathbb{Z}_3^{\otimes} \times \mathbb{Z}_3^{\otimes} \to \mathbb{Z}_3^{\otimes}$ given by $a \star b = (a^b) \bmod 3$.
3. ___ The operation $\oplus : \mathbb{Z}_3 \times \mathbb{Z}_3 \to \mathbb{Z}_3$ 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 $\otimes : \mathbb{Z}_{11} \times \mathbb{Z}_{11} \to \mathbb{Z}_{11}$ 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 $\ominus : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ 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 $\star : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ be given by $a \star b = \left(a^b\right)$.

[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 subraction

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 $b \in \mathbb{Z}_1 1$ 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 form these operations on the integers. One of the 'inherited' properties is the identity element.

In the cases were 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 × S → 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 $(a,b) \oplus (c,d) = ((a+c) \text{ mod } 3, (b+d) \text{ mod } 2)$:

$\oplus$	**(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 $(a,b) \oplus (c,d) = ((a+c) \text{ mod } 2, (b+d) \text{ mod } 2)$:

$\oplus$	**(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 $a \oplus b = (a+b)$ mod 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 $\oplus : \mathbb{Z}_4 \times \mathbb{Z}_4 \to \mathbb{Z}_4$ 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 $\otimes : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ 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 $\oplus : \mathbb{Z}_4 \times \mathbb{Z}_4 \to \mathbb{Z}_4$ 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 × S → S be a binary operation on S. We read a * b as 'a star b'.

The operation * is commutative if $\underline{\quad (A) \quad}$ for $\underline{\quad (B) \quad}$.

(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 $a \otimes b = (a \cdot b)$ mod 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 $\oplus : \mathbb{Z}_7 \times \mathbb{Z}_7 \to \mathbb{Z}_7$ given by $a \oplus b = (a+b)$ mod 7.
2. ___ The operation $\ominus : \mathbb{Z}_{14} \times \mathbb{Z}_{14} \to \mathbb{Z}_{14}$ given by $a \ominus b = (a-b)$ mod 14.
3. ___ The operation $\otimes : \mathbb{Z}_5^{\otimes} \times \mathbb{Z}_5^{\otimes} \to \mathbb{Z}_5^{\otimes}$ given by $a \otimes b = (a \cdot b)$ mod 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 $\star : \mathbb{Z}_5 \times \mathbb{Z}_5 \to \mathbb{Z}_5$ be given by $a \star b = \left(a^b\right) \bmod 5$.

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 $\oplus : \mathbb{Z}_{15} \times \mathbb{Z}_{15} \to \mathbb{Z}_{15}$ 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 $\otimes : \mathbb{Z}_{11} \times \mathbb{Z}_{11} \to \mathbb{Z}_{11}$ 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

  $$a \star 3 = 2 \star 3 = 2^3 \text{ mod } 5 = 8 \text{ mod } 5 = 3$$

  and

  $$3 \star a = 3 \star 2 = 2^3 \text{ mod } 5 = 9 \text{ mod } 5 = 4$$

  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 $\underline{\quad(A)\quad}$ for $\underline{\quad(B)\quad}$.

(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 $\underline{\quad(A)\quad}$ for $\underline{\quad(B)\quad}$.

(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 $\underline{\quad(A)\quad}$ for $\underline{\quad(B)\quad}$.

(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 $\underline{\quad(A)\quad}$ with respect to * in S and $\underline{\quad(B)\quad}$ with respect to * in S and $\underline{\quad(C)\quad}$.

(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 $\star : G \times G \to G$ 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 $\left(\mathbb{Z}_3^{\otimes}, \otimes\right)$ 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 $(a,b)\star(c,d) = \big((a+c) \bmod 2, (b+d) \bmod 3\big)$:

$\star$	**(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 $\Box$.

(3) The operation $\Box$ is associative.

(4) The operation $\Box$ is ___.
[select: | **commutative** | **not commutative**]

Conclude whether $(D,\Box)$ is a commutative group:

The set D with the operation $\Box$ 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:

$a \bmod 7 =$ _____
$b \bmod 7 =$ _____
$c \bmod 7 =$ _____
$d \bmod 7 =$ _____

Now use these to compute the following:

$(a+b) \bmod 7 =$ _____
$(c+d) \bmod 7 =$ _____
$(b \cdot c) \bmod 7 =$ _____
$(d \cdot a) \bmod 7 =$ _____

Problem 14.3 (2) (1 point)

Perform the following computations:

$2103 \bmod 11 =$ _____
$5313 \bmod 11 =$ _____
$8983 \bmod 11 =$ _____

Now use these results to find the following:

$(2103 \cdot 5313) \bmod 11 =$ _____
$(5313 + 8983) \bmod 11 =$ _____
$((2103 \cdot 5313) + 8983) \bmod 11 =$ _____
$(2103 + 5313 + 8983) \bmod 11 =$ _____

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:

$(a+a) \bmod 8 =$ ___

$(a+b)$ mod 8 = ___

$(a \cdot b)$ mod 8 = ___

$(a+3)$ mod 8 = ___

$(3 \cdot b)$ mod 8 = ___

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:

$(a+a)$ mod 42 = ___

$(a+b)$ mod 42 = ___

$(a \cdot b)$ mod 42 = ___

$(a+10)$ mod 42 = ___

$(10 \cdot b)$ mod 42 = ___

Problem 14.3 (5) (1 point)

Let $\oplus : \mathbb{Z}_{47} \times \mathbb{Z}_{47} \to \mathbb{Z}_{47}$ be defined by $a \oplus b = (a+b) \bmod 47$.

Compte

$9 \oplus 45 =$ ___

$45 \oplus 9 =$ ___

$(22 \oplus 21) \oplus 17 =$ ___

$22 \oplus (21 \oplus 17) =$ ___

Problem 14.3 (6) (1 point)

Let $\otimes : \mathbb{Z}_{11}^{\otimes} \times \mathbb{Z}_{11}^{\otimes} \to \mathbb{Z}_{11}^{\otimes}$ be defined by $a \otimes b = (a \cdot b) \bmod 11$.

Compute

$8 \otimes 9 =$ ___

$4 \otimes 3 =$ ___

$10 \otimes 6 =$ ___

$7 \otimes 9 =$ ___

$(3 \otimes 1) \otimes 8 =$ ___

$3 \otimes (1 \otimes 8) =$ ___

Problem 14.3 (7) (1 point)

What is the identity in the following sets with respect to the given operation.

1. ___ $\mathbb{Z}_4$ with the operation * defined by $a * b = (a \cdot b)$ mod 4
2. ___ $\mathbb{Z}$ with the operation * defined by $a * b = a \cdot b$
3. ___ $\mathbb{Z}$ with addition
4. ___ $\mathbb{Z}_4$ with the operation * defined by $a * b = (a + b)$ mod 4
5. ___ $\mathbb{Z}_2^{\otimes}$ with the operation * defined by $a * b = (a \cdot b)$ mod 2

Problem 14.3 (8) (1 point)

Consider the binary operation $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$.

The identity with respect to $+$ in $\mathbb{Z}$ is ___.
The inverse of 39 with respect to $+$ in $\mathbb{Z}$ is ___.

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 form these operations on the integers. One of the 'inherited' properties is the identity element.

In the cases were 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

$\oplus : \mathbb{Z}_{22} \times \mathbb{Z}_{22} \to \mathbb{Z}_{22}$ defined by $a \oplus b = a + b$ mod 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=$\{0,1,2,3,...,m-1\}$. Let ⊕:S×S→S be given by a⊕b=(a+b) mod m.

We show that (S,⊕) is a group.

(a) Because a⊕0 = $\underline{\quad (A) \quad}$ and 0⊕a = $\underline{\quad (B) \quad}$ for all a in S, the element $\underline{\quad (C) \quad}$ is the $\underline{\quad (D) \quad}$ with respect to the operation ⊕.

(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⊕ $\underline{\quad (A) \quad}$ = 0 and $\underline{\quad (B) \quad}$ ⊕a = 0.
Thus each a in S has an $\underline{\quad (C) \quad}$ with respect to the operation ⊕.

(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 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) mod m** | **(a+(b+c)) mod m** | **(a+b) mod m** | **(b+a) mod m** | **(a(b+c)) mod m** | **(ab+ac) mod m**]

(C): [select: | **((a+b)+c) mod m** | **(a+(b+c)) mod m** | **(a+b) mod m** | **(b+a) mod m** | **(a(b+c)) mod m** | **(ab+ac) mod 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 for all a and b in S we have a⊕b = $\underline{\quad (B) \quad}$ = $\underline{\quad (C) \quad}$ = b⊕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) mod m** | **(a+(b+c)) mod m** | **(a+b) mod m** | **(b+a) mod m** | **(a(b+c)) mod m** | **(ab+ac) mod m**]

(C): [select: | **((a+b)+c) mod m** | **(a+(b+c)) mod m** | **(a+b) mod m** | **(b+a) mod m** | **(a(b+c)) mod m** | **(ab+ac) mod m**]

Hence the operation ⊕ is ___.
[select: | **associative** | **commutative** | **disruptive** | **distributive** | **orderly**]

We have shown that

(a) the set S contains an identity with respect to the operation ⊕,
(b) for each element in S the set S contains an inverse with respect to ⊕,
(c) the operation ⊕ is associative,
(d) the operation ⊕ is commutative.

Thus the set S with the operation ⊕ 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) mod m
- (a+(b+c)) mod m
- associative
- a+b = b+a
- (a+b) mod m
- (b+a) mod 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 $\left(\mathbb{Z}_7^{\otimes}, \otimes\right)$ 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

$\oplus : \mathbb{Z}_{20} \times \mathbb{Z}_{20} \to \mathbb{Z}_{20}$ defined by $a \oplus b = a + b$ mod 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 $a \otimes b = (a \cdot b)$ mod 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 $a \otimes b = (a \cdot b)$ mod 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

$\otimes : \mathbb{Z}_3^{\otimes} \times \mathbb{Z}_3^{\otimes} \to \mathbb{Z}_3^{\otimes}$ defined by $a \otimes b = a \cdot b$ mod 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,...,p-1. Let $\otimes$:S$\times$S$\to$S be given by a$\otimes$b=(a$\cdot$b) mod p.

We show that (S,$\otimes$) is a group.

(a) Because a$\otimes$1 = ___(A)___ and 1$\otimes$a = ___(B)___ for all a in S, the element ___(C)___ is the ___(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,...,p-1. As p is prime we have gcd(a,p) = ___(A)___.
By Bezout's theorem there are integers s and t such that s$\cdot$a+t$\cdot$p = ___(B)___.
Thus ___(C)___ $\otimes$a = (___(D)___ $\cdot$ a) mod p =1.
So ___(E)___ mod p is the ___(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 for all a, b, and c in S we have (a$\otimes$b)$\otimes$ c =((a$\cdot$b)$\cdot$ c) mod p =(a$\cdot$(b$\cdot$ c)) mod p =a$\otimes$(b$\otimes$ c).

[select: | **associative** | **commutative** | **disruptive** | **distributive** | **negative** | **orderly** | **positive** |

transitive]

Hence the operation ⊗ is ______.

[select: | **associative** | **commutative** | **disruptive** | **distributive** | **negative** | **orderly** | **positive** | **transitive**]

(d) The multiplication of integers is ______, that is, a·b=b·a for all integers a and b. Thus for all a and b in S we have a⊗b =(a·b) mod p =(b·a) mod p =b⊗a.

[select: | **associative** | **commutative** | **disruptive** | **distributive** | **negative** | **orderly** | **positive** | **transitive**]

Hence the operation ⊗ 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 ⊗,
[select: | **analogue** | **identity** | **inverse** | **opposite** | **unit**]

(b) for each element in S the set S contains an ______ with respect to ⊗,
[select: | **analogue** | **identity** | **inverse** | **opposite** | **unit**]

(c) the operation ⊗ is associative,

(d) the operation ⊗ 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:

$4^{0\otimes} =$ ___

$4^{1\otimes} =$ ___

$4^{2\otimes} =$ ___

$4^{3\otimes} =$ ___

$4^{4\otimes} =$ ___

Use the information above to find the smallest non-negative integer n such that $4^{n\otimes} = 1$.

$n =$___

Problem 15.1 (2) (1 point)

In $(\mathbb{Z}_7^{\otimes}, \otimes)$ where $a \otimes b := (a \cdot b) \bmod 7$ compute:

$5^{0\otimes} =$ ___

$5^{1\otimes} =$ ___

$5^{2\otimes} =$ ___

$5^{3\otimes} =$ ___

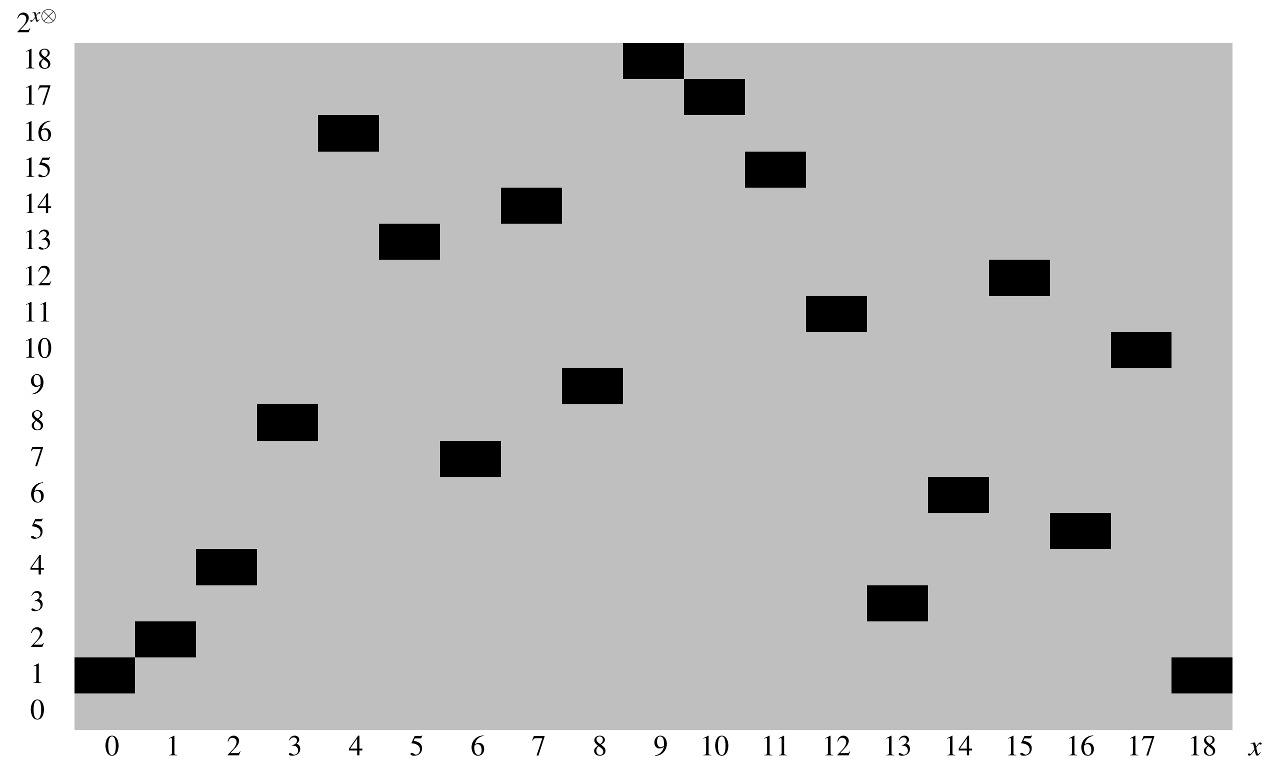
$5^{4\otimes} =$ ___

$5^{5\otimes} =$ ___

$5^{6\otimes} =$ ___

Problem 15.1 (3) (1 point)

We consider the function $h : \mathbb{Z}_{19} \to \mathbb{Z}_{19}$ given by $h(x) = 2^{x\otimes} = 2^x \bmod 19$.



Find the following:

$2^{0\otimes} =$ ___

$2^{3\otimes} =$ ___

$2^{5\otimes} =$ ___

$2^{7\otimes} =$ ___

$2^{8\otimes} =$ ___

$2^{9\otimes} =$ ___

$2^{11\otimes} =$ ___

$2^{14\otimes} =$ ___

$2^{18\otimes} =$ ___

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

$$b^{n\otimes} = \underbrace{b \otimes b \otimes \cdots \otimes b}_{\text{n times}}.$$

In $(\mathbb{Z}_{17}^{\otimes}, \otimes)$ where $a \otimes b = (a \cdot b) \bmod 17$ compute:

$1^{2\otimes} =$ ___

$2^{4\otimes} =$ ___

$4^{2\otimes} =$ ___

$5^{2\otimes} =$ ___

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.

___ 1. $a^{3\otimes}$	A. $a^{2\otimes}$
___ 2. $a^{(n+m)\otimes}$	B. a
___ 3. $a^{1\otimes}$	C. $a^{n\otimes} \otimes a^{m\otimes}$
___ 4. $(a^{n\otimes})^{m\otimes}$	D. $a^{(n\cdot m)\otimes}$
___ 5. $a \otimes a$	E. 1
___ 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 $b :=$ ___ an exponent $n :=$ ___ and a modulus $m :=$ ___.

let $c := 3$ and **let** $i := 1$.

let $c := (c \cdot 3) \bmod 19 = \_\_\_$ and **let** $i := i+1 = \_\_\_$

let $c := (c \cdot 3) \bmod 19 = \_\_\_$ and **let** $i := i+1 = \_\_\_$

let $c := (c \cdot 3) \bmod 19 = \_\_\_$ and **let** $i := i+1 = \_\_\_$

let $c := (c \cdot 3) \bmod 19 = \_\_\_$ and **let** $i := i+1 = \_\_\_$

let $c := (c \cdot 3) \bmod 19 = \_\_\_$ and **let** $i := i+1 = \_\_\_$

let $c := (c \cdot 3) \bmod 19 = \_\_\_$ and **let** $i := i+1 = \_\_\_$

let $c := (c \cdot 3) \bmod 19 = \_\_\_$ and **let** $i := i+1 = \_\_\_$

let $c := (c \cdot 3) \bmod 19 = \_\_\_$ and **let** $i := i+1 = \_\_\_$

let $c := (c \cdot 3) \bmod 19 = \_\_\_$ and **let** $i := i+1 = \_\_\_$

let $c := (c \cdot 3) \bmod 19 = \_\_\_$ and **let** $i := i+1 = \_\_\_$

let $c := (c \cdot 3) \bmod 19 = \_\_\_$ and **let** $i := i+1 = \_\_\_$

let $c := (c \cdot 3) \bmod 19 = \_\_\_$ and **let** $i := i+1 = \_\_\_$

let $c := (c \cdot 3) \bmod 19 = \_\_\_$ and **let** $i := i+1 = \_\_\_$

let $c := (c \cdot 3) \bmod 19 = \_\_\_$ and **let** $i := i+1 = \_\_\_$

Because the statement $i = 15$ is true, the loop ends here.

Output: $3^{15} \bmod 19 = c = \_\_\_$.

Problem 15.1 (7) (1 point)

In $(\mathbb{Z}_{13}^{\otimes}, \otimes)$ where $a \otimes b := (a \cdot b) \bmod 13$ compute:

$3^{0\otimes} = \_\_\_$
$3^{1\otimes} = \_\_\_$

$$3^{2\otimes} = 3^{(1+1)\otimes} = 3^{1\otimes} \otimes 3 = \_\_\_ \otimes 3 = \left(\_\_\_ \cdot 3\right) \bmod 13 = \_\_\_$$

$$3^{3\otimes} = 3^{(2+1)\otimes} = 3^{2\otimes} \otimes 3 = \_\_\_ \otimes 3 = \left(\_\_\_ \cdot 3\right) \bmod 13 = \_\_\_$$

$$3^{4\otimes} = 3^{(3+1)\otimes} = 3^{3\otimes} \otimes 3 = \_\_\_ \otimes 3 = \left(\_\_\_ \cdot 3\right) \bmod 13 = \_\_\_$$

$$3^{5\otimes} = 3^{(4+1)\otimes} = 3^{4\otimes} \otimes 3 = \_\_\_ \otimes 3 = \left(\_\_\_ \cdot 3\right) \bmod 13 = \_\_\_$$

$$3^{6\otimes} = 3^{(5+1)\otimes} = 3^{5\otimes} \otimes 3 = \_\_\_ \otimes 3 = \left(\_\_\_ \cdot 3\right) \bmod 13 = \_\_\_$$

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

$$5^{3\otimes} = 5^{(2+1)\otimes} = 5^{2\otimes} \otimes 5 = 4 \otimes 5 = \big(4 \cdot 5\big) \bmod 7 = 6.$$

Correct Answers:

- 1
- 5
- 4
- 6
- 2
- 3
- 1

Problem 15.1 (3) *Correct Answers:*

Hint: The graph of the function $h : \mathbb{Z}_{19} \to \mathbb{Z}_{19}$ 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

$$3^{3\otimes} = 3^{(2+1)\otimes} = 3^{2\otimes} \otimes 3 = 9 \otimes 3 = \big(9 \cdot 3\big) \bmod 13 = 27 \bmod 13 = 1.$$

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

$$b^{n\otimes} = \underbrace{b \otimes b \otimes \cdots \otimes b}_{\text{n copies of b}}.$$

In $(\mathbb{Z}_{41}^{\otimes}, \otimes)$ where $a \otimes b = (a \cdot b) \bmod 41$ follow these steps to compute $5^{32\otimes}$.

$5^{1\otimes} =$ ___

$5^{2\otimes} = 5^{1\otimes} \otimes 5^{1\otimes} =$ ___$\otimes$___=___

$5^{4\otimes} = 5^{2\otimes} \otimes 5^{2\otimes} =$ ___$\otimes$___=___

$5^{8\otimes} = 5^{4\otimes} \otimes 5^{4\otimes} =$ ___$\otimes$___=___

$5^{16\otimes} = 5^{8\otimes} \otimes 5^{8\otimes} =$ ___$\otimes$___=___

$5^{32\otimes} = 5^{16\otimes} \otimes 5^{16\otimes} =$ ___$\otimes$___=___

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 $\otimes : \mathbb{Z}_{19937}^{\otimes} \times \mathbb{Z}_{19937}^{\otimes} \to \mathbb{Z}_{19937}^{\otimes}$ 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

$$b^{n\otimes} := \underbrace{b \otimes b \otimes \cdots \otimes b}_{\text{n copies of b}}.$$

How many operations $\otimes$ are needed to compute $3^{8\otimes}$ with the **naive** 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.

Naive Exponentiation

The first naive 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.

Example.

To find x^4 it requires 3 multiplications, namely (x with itself to find x^2, x with x^2 to find x^3 and finally x with x^3 to find x^4.)

Repeated Squaring

On the other hand there is also a second method called fast exponentiation where we at each stage multiply the last number with itself.

Example.

To find x^4, one first multiplies x with itself to get x^2, then one multiplies x^2 with itself to get x^4. This second method only took 2 multiplications to find x^4.

Questions

To calculate x^{128} with the naive exponentiation method takes _____ multiplications.

To calculate x^{128} with the repeated squaring method takes _____ multiplications.

Which method is more efficient ?

- A. Naive exponentiation is more efficient than fast exponentiation.
- B. Repeated squaring is more efficient than naive exponentiation.

Problem 15.2 (5) (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

$$b^{n\otimes} = \underbrace{b \otimes b \otimes \cdots \otimes b}_{\text{n copies of b}}.$$

In $(\mathbb{Z}_{83}^{\otimes}, \otimes)$ where $a \otimes b = (a \cdot b) \bmod 83$ we have

$7^{8\otimes} = 36.$

Compute

$7^{16\otimes} = 7^{8\otimes} \otimes 7^{8\otimes} =$ ___$\otimes$___=___

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

$$b^{n\otimes} = \underbrace{b \otimes b \otimes \cdots \otimes b}_{\text{n copies of b}}.$$

In $(\mathbb{Z}_{83}^{\otimes},\otimes)$ where $a \otimes b = (a \cdot b) \bmod 83$ follow these steps to compute $5^{32\otimes}$.

$5^{1\otimes} =$ ___

$5^{2\otimes} = 5^{1\otimes} \otimes 5^{1\otimes} =$ ___$\otimes$___=___

$5^{4\otimes} = 5^{2\otimes} \otimes 5^{2\otimes} =$ ___$\otimes$___=___

$5^{8\otimes} = 5^{4\otimes} \otimes 5^{4\otimes} =$ ___$\otimes$___=___

$5^{16\otimes} = 5^{8\otimes} \otimes 5^{8\otimes} =$ ___$\otimes$___=___

$5^{32\otimes} = 5^{16\otimes} \otimes 5^{16\otimes} =$ ___$\otimes$___=___

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

$$b^{n\otimes} = \underbrace{b \otimes b \otimes \cdots \otimes b}_{\text{n copies of b}}.$$

In $(\mathbb{Z}_{79}^{\otimes},\otimes)$ where $a \otimes b = (a \cdot b) \bmod 79$ we have

$5^{16\otimes} = 31.$

Compute

$5^{32\otimes} = 5^{16\otimes} \otimes 5^{16\otimes} =$ ___$\otimes$___=___

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

$$b^{n\otimes} = \underbrace{b \otimes b \otimes \cdots \otimes b}_{\text{n copies of b}}.$$

In $(\mathbb{Z}_{103}^{\otimes}, \otimes)$ where $a \otimes b = (a \cdot b) \bmod 103$ follow these steps to compute $15^{64\otimes}$.

$15^{1\otimes} =$ ___

$15^{2\otimes} =$ ___

$15^{4\otimes} =$ ___

$15^{8\otimes} =$ ___

$15^{16\otimes} =$ ___

$15^{32\otimes} =$ ___

$15^{64\otimes} =$ ___

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:

$2^{18} \bmod 181 =$___

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:

$6^6 \bmod 251 =$___

Problem 15.3 (3) (1 point)

Fast Exponentiation

With the fast exponentiation algorithm find 4^8 mod 19.

Input: Base $b :=$ ___ an exponent $n :=$ ___ and a modulus $m :=$ ___.

---

let $a := 1$ and **let** $c := b =$ ___.

let $r := n \bmod 2 =$ ___. **if** $r = 1$ **then let** $a := (a \cdot c) \bmod 19$. Now $a =$___
let $n := n \operatorname{div} 2 =$ ___
and **let** $c := (c \cdot c) \bmod 19 =$___

let $r := n \bmod 2 =$ ___. **if** $r = 1$ **then let** $a := (a \cdot c) \bmod 19$. Now $a =$___
let $n := n \operatorname{div} 2 =$ ___
and **let** $c := (c \cdot c) \bmod 19 =$___

let $r := n \bmod 2 =$ ___. **if** $r = 1$ **then let** $a := (a \cdot c) \bmod 19$. Now $a =$___
let $n := n \operatorname{div} 2 =$ ___
and **let** $c := (c \cdot c) \bmod 19 =$___

let $r := n \bmod 2 =$ ___. **if** $r = 1$ **then let** $a := (a \cdot c) \bmod 19$. Now $a =$___
let $n := n \operatorname{div} 2 =$ ___

Because the statement $n = 0$ is true, the loop ends here.

Output: $4^8 \bmod 19 = a =$ ___.

Problem 15.3 (4) (1 point)

Let $\otimes : \mathbb{Z}_{41}^{\otimes} \times \mathbb{Z}_{41}^{\otimes} \to \mathbb{Z}_{41}^{\otimes}$ 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.

$48 = (\;\_\_\_ \cdot 64) + (\;\_\_\_ \cdot 32) + (\;\_\_\_ \cdot 16) + (\;\_\_\_ \cdot 8) + (\;\_\_\_ \cdot 4) + (\;\_\_\_ \cdot 2) + (\;\_\_\_ \cdot 1)$

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.

$9^{1\otimes} =$ ___	[select: | **yes** | **no**]
$9^{2\otimes} = 9^{1\otimes} \otimes 9^{1\otimes} =$ ___	[select: | **yes** | **no**]
$9^{4\otimes} = 9^{2\otimes} \otimes 9^{2\otimes} =$ ___	[select: | **yes** | **no**]
$9^{8\otimes} = 9^{4\otimes} \otimes 9^{4\otimes} =$ ___	[select: | **yes** | **no**]
$9^{16\otimes} = 9^{8\otimes} \otimes 9^{8\otimes} =$ ___	[select: | **yes** | **no**]
$9^{32\otimes} = 9^{16\otimes} \otimes 9^{16\otimes} =$ ___	[select: | **yes** | **no**]
$9^{64\otimes} = 9^{32\otimes} \otimes 9^{32\otimes} =$ ___	[select: | **yes** | **no**]

Use these values to compute $9^{48\otimes}$

$9^{48\otimes} =$ _____

Problem 15.3 (5) (1 point)

Let $\otimes : \mathbb{Z}_{11}^{\otimes} \times \mathbb{Z}_{11}^{\otimes} \to \mathbb{Z}_{11}^{\otimes}$ 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.

$4 = (\ \_\_\_ \cdot 16) + (\ \_\_\_ \cdot 8) + (\ \_\_\_ \cdot 4) + (\ \_\_\_ \cdot 2) + (\ \_\_\_ \cdot 1)$

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.

$5^{1\otimes} =$ ___	[select: | **yes** | **no**]
$5^{2\otimes} = 5^{1\otimes} \otimes 5^{1\otimes} =$ ___	[select: | **yes** | **no**]
$5^{4\otimes} = 5^{2\otimes} \otimes 5^{2\otimes} =$ ___	[select: | **yes** | **no**]
$5^{8\otimes} = 5^{4\otimes} \otimes 5^{4\otimes} =$ ___	[select: | **yes** | **no**]
$5^{16\otimes} = 5^{8\otimes} \otimes 5^{8\otimes} =$ ___	[select: | **yes** | **no**]

Use the above to compute $5^{4\otimes}$

$5^{4\otimes} =$ _____

Problem 15.3 (6) (1 point)

Let $\otimes : \mathbb{Z}_{37}^{\otimes} \times \mathbb{Z}_{37}^{\otimes} \to \mathbb{Z}_{37}^{\otimes}$ be given by $a \otimes b = (a \cdot b) \bmod 37$. Compute

$$7^{15\otimes} = \underbrace{7 \otimes \cdots \otimes 7}_{\text{15 copies of 7}} = 7^{15} \bmod 37.$$

using that $7^{1\otimes} = 7$, $7^{2\otimes} = 12$, $7^{4\otimes} = 33$, $7^{8\otimes} = 16$.

$7^{15\otimes} =$ _____

Problem 15.3 (7) (1 point)

Let $\otimes : \mathbb{Z}_{1087}^{\otimes} \times \mathbb{Z}_{1087}^{\otimes} \to \mathbb{Z}_{1087}^{\otimes}$ 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:

$$3^{56\otimes} = \underbrace{3 \otimes \cdots \otimes 3}_{\text{56 copies of 3}} = 3^{56} \bmod 1087.$$

$3^{56\otimes} =$ _____

If the numbers become top big, compute ” mod 1087 ” after every multiplication.

Problem 15.3 (8) (1 point)

Let $\otimes : \mathbb{Z}_{73}^{\otimes} \times \mathbb{Z}_{73}^{\otimes} \to \mathbb{Z}_{73}^{\otimes}$ 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 $7^{33\otimes}$

$7^{33\otimes} =$ _____

Problem 15.3 (9) (1 point)

Let $\otimes : \mathbb{Z}_{23}^{\otimes} \times \mathbb{Z}_{23}^{\otimes} \to \mathbb{Z}_{23}^{\otimes}$ 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.

$33 = (\_\_\_ \cdot 64) + (\_\_\_ \cdot 32) + (\_\_\_ \cdot 16) + (\_\_\_ \cdot 8) + (\_\_\_ \cdot 4) + (\_\_\_ \cdot 2) + (\_\_\_ \cdot 1)$

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.

$5^{1\otimes} = 5$	[select: | **yes** | **no**]
$5^{2\otimes} = 2$	[select: | **yes** | **no**]
$5^{4\otimes} = 4$	[select: | **yes** | **no**]
$5^{8\otimes} = 16$	[select: | **yes** | **no**]
$5^{16\otimes} = 3$	[select: | **yes** | **no**]
$5^{32\otimes} = 9$	[select: | **yes** | **no**]
$5^{64\otimes} = 12$	[select: | **yes** | **no**]

Use the above to compute $5^{33\otimes}$.

$5^{33\otimes} =$ _____

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:

$4^{0\otimes} =$ ___

$4^{1\otimes} =$ ___

$4^{2\otimes} =$ ___

$4^{3\otimes} =$ ___

$4^{4\otimes} =$ ___

$4^{5\otimes} =$ ___

$4^{6\otimes} =$ ___

$4^{7\otimes} =$ ___

$4^{8\otimes} =$ ___

$4^{9\otimes} =$ ___

$4^{10\otimes} =$ ___

$4^{11\otimes} =$ ___

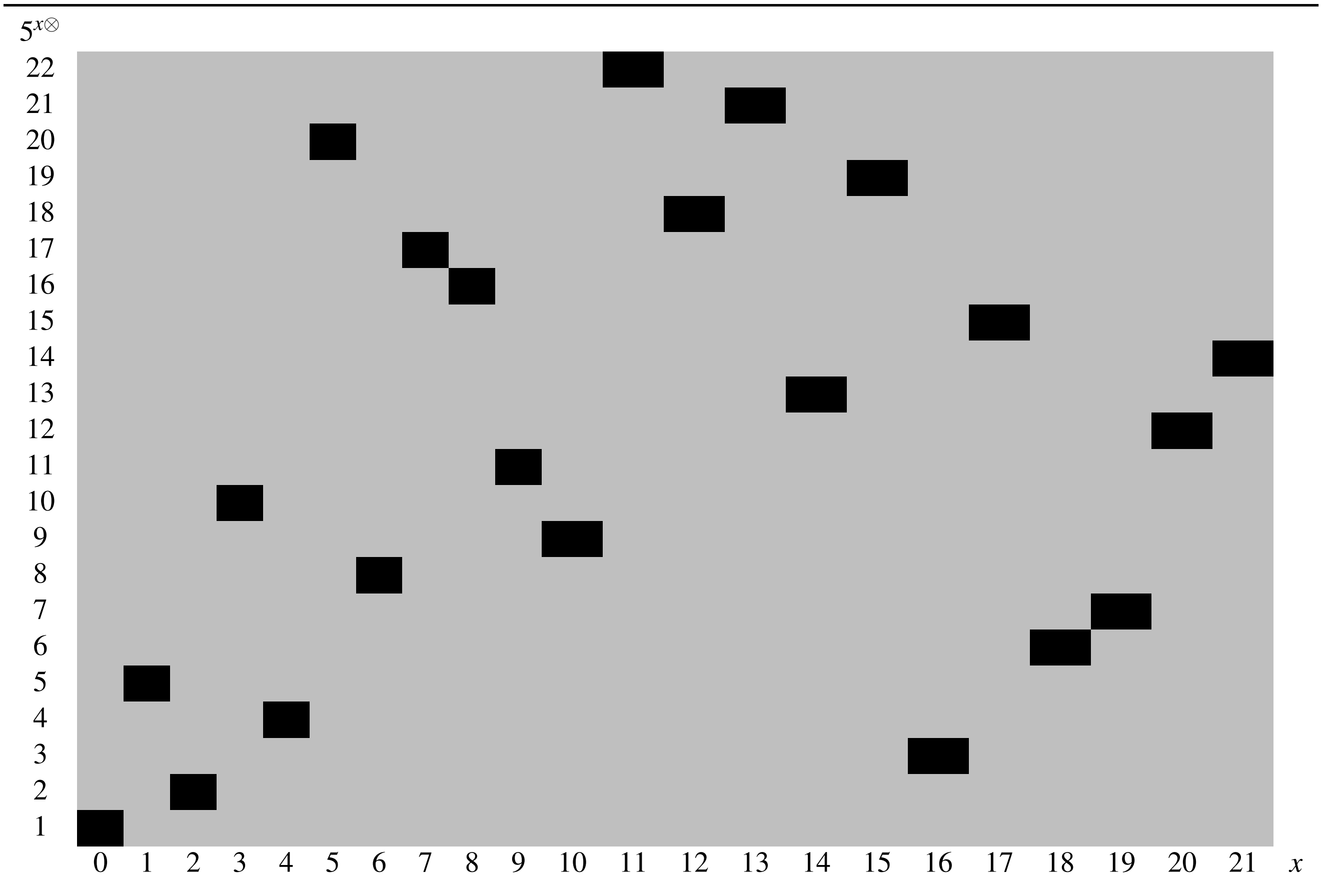
$4^{12\otimes} =$ ___

Use the information above to find the smallest non-negative integer n such that $4^{n\otimes} = 1$.

$n =$___

Problem 15.4 (2) (1 point)

Consider the function $g : \mathbb{Z}_{22} \to \mathbb{Z}_{23}^{\otimes}$ given by $g(x) = 5^{x\otimes} = 5^x \bmod 23$.



Find the following:

$\log_5^{\otimes}(1) =$ ___

$\log_5^{\otimes}(5) =$ ___

$\log_5^{\otimes}(9) =$ ___

$\log_5^{\otimes}(10) =$ ___

$\log_5^{\otimes}(14) =$ ___

$\log_5^{\otimes}(17) =$ ___

$\log_5^{\otimes}(20) =$ ___

Problem 15.4 (3) (1 point)

In $(\mathbb{Z}_{13}^{\otimes}, \otimes)$ where $a \otimes b = (a \cdot b) \bmod 13$ compute:

$7^{0\otimes} = \_\_\_$

$7^{1\otimes} = \_\_\_$

$7^{2\otimes} = \_\_\_$

$7^{3\otimes} = \_\_\_$

$7^{4\otimes} = \_\_\_$

$7^{5\otimes} = \_\_\_$

$7^{6\otimes} = \_\_\_$

$7^{7\otimes} = \_\_\_$

$7^{8\otimes} = \_\_\_$

$7^{9\otimes} = \_\_\_$

$7^{10\otimes} = \_\_\_$

$7^{11\otimes} = \_\_\_$

Now use the information above to find the following:

$\log_7^{\otimes} 1 = \_\_\_$

$\log_7^{\otimes} 2 = \_\_\_$

$\log_7^{\otimes} 3 = \_\_\_$

$\log_7^{\otimes} 4 = \_\_\_$

$\log_7^{\otimes} 5 = \_\_\_$

$\log_7^{\otimes} 6 = \_\_\_$

$\log_7^{\otimes} 7 = \_\_\_$

$\log_7^{\otimes} 8 = \_\_\_$

$\log_7^{\otimes} 9 = \_\_\_$

$\log_7^{\otimes} 10 = \_\_\_$

$\log_7^{\otimes} 11 = \_\_\_$

$\log_7^{\otimes} 12 = \_\_\_$

Problem 15.4 (4) (1 point)

In $(\mathbb{Z}_7^{\otimes}, \otimes)$ where $a \otimes b = (a \cdot b) \bmod 7$ compute:

$2^{0\otimes} = \_\_\_$

$2^{1\otimes} = \_\_\_$

$2^{2\otimes} = \_\_\_$

$2^{3\otimes} = \_\_\_$

$2^{4\otimes} = \_\_\_$

$2^{5\otimes} = \_\_\_$

$2^{6\otimes} = \_\_\_$

Now use the information above to find the following:

$\log_2^{\otimes}(1) = \_\_\_$

Problem 15.4 (5) (1 point)

Let $\otimes : \mathbb{Z}_{11}^{\otimes} \times \mathbb{Z}_{11}^{\otimes} \to \mathbb{Z}_{11}^{\otimes}$ 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.

$\log_7^{\otimes}(7) = \_\_\_\_\_$

Problem 15.4 (6) (1 point)

Let $\otimes : \mathbb{Z}_{17}^{\otimes} \times \mathbb{Z}_{17}^{\otimes} \to \mathbb{Z}_{17}^{\otimes}$ be given by $a \otimes b = (a \cdot b) \bmod 17$.

Find smallest non-negative integer n such that $14^{n\otimes} = 3$.

$n = \_\_\_\_\_$

Problem 15.4 (7) (1 point)

Let $\otimes : \mathbb{Z}_5^{\otimes} \times \mathbb{Z}_5^{\otimes} \to \mathbb{Z}_5^{\otimes}$ 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.

$\log_4^{\otimes}(4) =$ _____

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 $g : \mathbb{Z}_{23-1} \to \mathbb{Z}_{23}^{\otimes}$ given by $g(x) = 5^{x\otimes} = 5^x \bmod 23$ is

$$\{(x, 5^x \bmod 23) \mid x \in \mathbb{Z}_{22}\} \subseteq \mathbb{Z}_{22} \to \mathbb{Z}_{23}^{\otimes}$$

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 $663634 - 939021$ $\underline{\quad (A) \quad}$ computing $-275387 + 939021$. So subtraction is $\underline{\quad (B) \quad}$ 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 $\otimes : \mathbb{Z}_{19759} \times \mathbb{Z}^{\otimes}_{19759} \to \mathbb{Z}^{\otimes}_{19759}$ be given by $a \otimes b = (a \cdot b)$ mod 19759.

Computing $3^{14\otimes}$ $\underline{\quad (A) \quad}$ computing $\log^{\otimes}_3 1291$. So exponentiation modulo 19759 with the inverse discrete logarithm is $\underline{\quad (B) \quad}$ 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 $\underline{\quad (A) \quad}$ which he does not share with anyone and a(n) $\underline{\quad (B) \quad}$.

(A): [select: | **car key** | **house key** | **private key** | **public key**]

(B): [select: | **car key** | **house key** | **private key** | **public key**]

Bob publishes his $\underline{\quad (C) \quad}$ 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 $\underline{\quad (D) \quad}$ in the public key directory. She uses Bob's $\underline{\quad (E) \quad}$ to encrypt a(n) $\underline{\quad (F) \quad}$ and sends the $\underline{\quad (G) \quad}$ 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) $\underline{\quad (H) \quad}$ Bob decrypts it using his $\underline{\quad (I) \quad}$ to obtain the $\underline{\quad (J) \quad}$.

(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 $(\{1,2,3,\ldots,p-1\},*)$ 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 $\{1,2,3,\ldots,p-1\}$ and computes B := ________.

[select: | $g*a$ | $g*b$ | g^a | g^b | g^p | A^b | B^a]

Alices chooses an element a in $\{1,2,3,\ldots,p-1\}$ 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 $a \otimes b = (a \cdot b)$ mod 1759. They also agree on the generator $g = 6$.

Alice

Alice chooses her secret $a = 3$ and sends $A =$ ___ to Bob.

Bob

Bob chooses his secret $b = 2$ and sends $B =$ ___ to Alice.

Alice

Alice receives $B =$ ___ from Bob computes the shared secret ___.

Bob

Bob receives $A =$ ___ from Alice computes the shared secret ___.

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 ?

$B =$___.

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 $s =$___.

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 $A = g^{a\otimes} = (g^a) \bmod 19 =$ ___ to Bob.

Bob: Secret

Bob chooses his secret $b = 4$ and sends $B = g^{b\otimes} = (g^b) \bmod 19 =$ ___ to Alice.

Alice: Shared Secret

Alice receives $B =$ ___ from Bob, and she computes the shared secret $B^{a\otimes} = (B^a) \bmod 19 =$ ___.

Bob: Shared Secret

Bob receives $A =$ ___ from Alice, and he computes the shared secret $A^{b\otimes} = (A^b) \bmod 19 =$ ___.

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 $A = (g^a) \bmod p =$ ___ to Bob.

Bob: Secret

Bob chooses his secret $b = 5$ and sends $B = (g^b) \bmod p =$ ___ to Alice.

Alice: Shared Secret

Alice receives $B =$ ___ from Bob computes the shared secret $(B^a) \bmod p =$ ___.

Bob: Shared Secret

Bob receives $A =$ ___ from Alice computes the shared secret $(A^b) \bmod p =$ ___.

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 $A = g^{a\otimes} = (g^a) \bmod 13 = \_\_\_$ to Bob.

Bob: Secret

Bob chooses his secret $b = 4$ and sends $B = g^{b\otimes} = (g^b) \bmod 13 = \_\_\_$ to Alice.

Alice: Shared Secret

Alice receives $B = \_\_\_$ from Bob, and she computes the shared secret $B^{a\otimes} = (B^a) \bmod 13 = \_\_\_$.

Bob: Shared Secret

Bob receives $A = \_\_\_$ from Alice, and he computes the shared secret $A^{b\otimes} = (A^b) \bmod 13 = \_\_\_$.

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 $s =$___ 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 $(\{1,2,3,...,p-1\},*)$ where $a*b = (a \cdot b)$ mod p.

In the dropdown menus we write $g\hat{}c$ for g^{c*}.

Bob chooses an element b in $\{1,2,3,\ldots,p-1\}$ 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)]

Alices chooses a in $\{1,2,3,\ldots,p-1\}$ 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 $\{1,2,3,\ldots,p-1\}$ 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 $(\{1,2,3,...,p-1\},*)$.

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 $a\otimes b=(a\cdot b)$ mod 7. He chooses $g=3\in\mathbb{Z}_7^{\otimes}$.

Bob chooses his secret key $b=3$ and computes $B=(g^b)$ mod $p=$___.

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.

Alice gets Bob's public key from the directory: $p =$___, $g =$___, $B =$___

Alice chooses her secret $a = 2$.

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.

Bob: Decryption

Bob receives A and X from Alice.

Bob computes the shared secret $s = (A^b) \bmod p = \_\_\_$.

Bob finds the inverse $s^{-1\otimes} = \_\_\_$ of s in the group $(\mathbb{Z}_7^{\otimes}, \otimes)$.

Bob decrypts the message by computing $M = (X \cdot s^{-1}) \bmod p = \_\_\_$.

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 $B = (g^b) \bmod 7 = \_\_\_$.

Bob publishes p, g, and B in the public key directory.

Directory of Public Keys

Bob: $p = \_\_\_$, $g = \_\_\_$, $B = \_\_\_$

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 $s = (A^b) \bmod 7 = \_\_\_$.

Bob finds the inverse $s^{-1} = \_\_\_$ of s in the group $(\mathbb{Z}_7^{\otimes}, \otimes)$.

Bob decrypts the message by computing $M = (X \cdot s^{-1}) \bmod 7 =$ ___.

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 $B = (g^b) \bmod 19753 =$___.

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: $p =$___, $g =$___, $B =$___

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 $s = (A^b) \bmod 19753 =$ ___.

Bob computes the inverse $s^{-1} = 11561$ of s in the group $(\mathbb{Z}_{19753}^{\otimes}, \otimes)$.

Bob decrypts the message by computing $M = (X \cdot s^{-1}) \bmod 19753 =$ ___.

Bob finds the expanded base 27 form of M, namely $M =$___$\cdot 27^2 +$___$\cdot 27 +$___.

Decoding these numbers with C^{-1} yields the message ___.

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 $C : \{-, \mathtt{a}, \mathtt{b}, \mathtt{c}, \ldots \mathtt{z}\} \to \{0, 1, 2, 3, \ldots 26\}$ with $C(-) = 0$, $C(\mathtt{a}) = 1$, ..., $C(\mathtt{z}) = 26$ to the characters in message. She obtains $C(\mathtt{e}) =$___, $C(\mathtt{v}) =$___, and $C(\mathtt{e}) =$___.

She encodes this into one number by computing $m = C(\mathtt{e}) \cdot 27^2 + C(\mathtt{v}) \cdot 27 + C(\mathtt{e}) =$___.

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 $m =$___.

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 $s =$___.

Alice encrypts the message $m = 2$ and sends $A =$___ and $X =$___ 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 $B = (g^b) \bmod p =$___.

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: $p =$___, $g =$___, $B =$___

Sebastian: $p = 19891$, $g = 32$, $B = 7993$

Victoria: $p = 19919$, $g = 6864$, $B = 5492$

Alice: Encryption

Alice wants to send the message '`ale`' to Bob.

Alice gets Bob's public key from the directory: $p =$___, $g =$___, $B =$___

She applies the encoding function $C : \{-, \mathtt{a}, \mathtt{b}, \mathtt{c}, \ldots \mathtt{z}\} \to \{0, 1, 2, 3, \ldots 26\}$ with $C(-) = 0$, $C(\mathtt{a}) = 1$, $\ldots$, $C(\mathtt{z}) = 26$ to the characters in message. She obtains $C(\mathtt{a}) =$___, $C(\mathtt{l}) =$___, and $C(\mathtt{e}) =$___.

She encodes this into one number by computing $m = C(\mathtt{a}) \cdot 27^2 + C(\mathtt{l}) \cdot 27 + C(\mathtt{e}) =$___.

Alice chooses her secret $a = 2$.

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.

Bob: Decryption

Bob receives A and X from Alice.

Bob computes the shared secret $s = (A^b) \bmod p = \_\_\_$.

Bob computes the inverse $s^{-1} = 12439$ of s in the group $(\mathbb{Z}_{19927}^{\otimes}, \otimes)$.

Bob decrypts the message by computing $M = (X \cdot s^{-1}) \bmod p = \_\_\_$.

Bob finds the expanded base 27 form of M, namely $M = \_\_\_ \cdot 27^2 + \_\_\_ \cdot 27 + \_\_\_$.

Decoding these numbers with C^{-1} yields the message ___.

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