INTRODUCTION TO MODULAR ARITHMETIC

Part A

Division Algorithm: For any two integers **a** and **n,** where n is positive, there exist unique integers **k** and **r** such that

$$a = \boldsymbol{k} \cdot n + \boldsymbol{r} \quad \text{and} \quad 0 \le r \le n - 1.$$

Examples

i. If $a = 15$ and $n = 2$, then $15 = 7 \cdot 2 + 1$, where $k = 7$ and $r = 1$.
ii. If $a = 138$ and $n = 15$, then $138 = 9 \cdot 15 + 3$, where $k = 9$ and $r = 3$.

Activity 1

A.

1) Fill in the following table.

a	n	k	r
5	12		
13	12		
18	12		
20	12		
24	12		
37	12		
42	12		
44	12		

2) Does it remind you any calculations that we might need to do in our daily lives?

B. Fill in the following table**.**

a	n	k	r
59			5
77			5

11			5
26			5

C. Determine a common "n" for the following set of numbers so that they all have the same remainder, which is "8"?
17, 24, 38, 52

PART B

MODULAR ARITHMETIC

Definition: If n is a positive integer, then

$$\boldsymbol{a}\ mod\ \boldsymbol{n}$$

is the remainder **r** obtained when a is divided by n according to the division algorithm and it is denoted by
$\boldsymbol{a}\ mod\ \boldsymbol{n} = \boldsymbol{r}$ *or* $\boldsymbol{a} \equiv \boldsymbol{r}\ mod(\boldsymbol{n})$ **.**

Examples

a) $55\ mod\ 4$
By the division algorithm, $55 = 13 \cdot 4 + 3$, so the remainder of 55when divided by 4 is 3.That is, we can say $55 \equiv 3\ mod(4)$ or $55\ mod\ 4 = 3$.

b) $245\ mod\ 35$
We have $245 = 7 \cdot 35 + 0$, and therefore $245\ mod\ 35 = 0$.

c) $58\ mod\ 7$
We have $58 = 8 \cdot 7 + 2$, we have $58 \equiv 2\ mod(7)$

d) $-43\ mod\ 5$
Since $-43 = (-9) \cdot 5 + 2$, we have $-43 \equiv 2\ mod(5)$.

e) $-4\ mod\ 7$
Since $-4 = (-5) \cdot 7 + 3$, we have $-4\ mod\ 7 = 3$.

Activity 2

A. Evaluate each of the following quantities.

i. $37 \ mod \ 52 =$

ii. $25 \ mod \ 7 =$

iii. $-2 \ mod \ 5 =$

iv. $87 \ mod \ 53 =$

v. $64 \ mod \ 7 =$

vi. $-24 \ mod \ 50 =$

Clock Arithmetic

The 12-hour clock system is based on an ordinary clock face, except that 12 is replaced by 0, so that the finite set of the system is S= {0, 1, 2, …, 11}.

Evaluate the following expressions in 12-hour clock system.

a) 8+5
b) 7+6
c) 3+9

The identity element is 0, that is a+0=a for each a in S.

Additive inverse: a+(-a)=0, for each a in S.

Example: 11+1=0, therefore -11=1

Activity 3

i. Determine the additive inverse, if it exists for each of the numbers in Clock Arithmetic.

a) 8
b) 3
c) 4
d) -5

ii) Do you see any similarities between clock arithmetic and modular arithmetic? Describe the relation if any.

Resources

Lewand, R. (2000). Cryptological mathematics. The mathematical Association of America.

Shodor. (2014). Retrieved from http://www.shodor.org/interactivate/lessons/ModularArithmetic/