MODULAR ARITHMETIC

- Kelvin Asclepius Minor –

1. The Division Theorem states that for two positive integers a and b, there exist unique numbers q and r such that $b = a \times q + r$. This theorem provides a fundamental understanding of how integers can be divided to produce a quotient q and a remainder r. What kind of integers are q and r?
2. In the Division Theorem $b = a \times q + r$, what kind of condition for b to be divisible by a $(a|b)$?
3. In the Division Theorem $b = a \times q + r$, what happened if a is a negative integer?
4. In the Division Theorem $b = a \times q + r$, what happened if b is a negative integer?
5. If a and b are positive integers, how many positive integers not exceeding a are divisible by b?
6. Given 3 integers a, b, and c, if $a|b$ and $a|c$, is $a|(b + c)$?
7. Given 3 integers a, b, and c, if $a|b$ and $a|c$, is $a|(b - c)$?
8. Given 3 integers a, b, and c, if $a|b$, is $a|(bc)$?
9. Given 3 integers a, b, and c, if $a|b$ and $b|c$, is $a|c$?
10. Given 5 integers a, b, c, d, and e, if $a|b$ and $b|c$, is $a|(db + ec)$?
11. Modular Arithmetic relies on the concept of remainders in $b = a \times q + r$. In Modular Arithmetic, two integers are said to be congruent modulo a $(mod\ a)$ if they have the same remainder when divided by a. What are two integers that are said to be congruent modulo a in the equation $b = a \times q + r$?
12. Find the congruence of 10 modulo 3 !
13. Find the congruence of 24 modulo 5 !
14. Find the congruence of 3 modulo 5 !
15. Find the congruence of 8 modulo 7 !
16. Find the congruence of -4 modulo 3 !
17. Find the congruence of 0 modulo 2 !
18. Find the congruence of 13 modulo 11 !
19. Find the congruence of -5 modulo 12 !
20. Find the congruence of 40 modulo 17 !

MODULAR ARITHMETIC

- Kelvin Asclepius Minor –

21. Applying the concept of Modular Arithmetic can lead to the creation of a new set of integers known as the set of equivalence classes modulo a $\mathbb{Z}_a = \{0, 1, 2, 3, \dots, a-1\}$. Write the elements of $\mathbb{Z}_{12}$!
22. In Modular Arithmetic, the Additive Inverse of number b modulo a is number b^{-1} such that $b + b^{-1} \equiv 0 \ (mod\ a)$. Find the Additive Inverse of 4 modulo 9 and the Additive Inverse of -5 modulo 12 !
23. In Modular Arithmetic, the Multiplicative Inverse of number b modulo a is number b^{-1} such that $b \times b^{-1} \equiv 1 \ (mod\ a)$. Determine whether the Multiplicative Inverse of 3 modulo 13 are 9, 18, 22, and 35 !
24. A Prime Number is a natural number greater than 1 that has no positive divisors other than 1 and the number itself, in contrast to a Composite Number, which is a natural number greater than 1 that has more than two positive divisors other than 1 and itself. Trial Division is one of the methods to determine whether a number is prime by testing divisibility by all prime numbers less than or equal to the square root of the number. If the number is divisible by any of these primes, then it is a Composite Number, otherwise it is a Prime Number. Why does Trial Division only check potential divisors up to the square root of the number?
25. Determine whether 11, 28, 29, 91, 97, 123, and 149 are Prime Numbers !
26. An integer d is a Divisor of another integer n if $d|n$, find the factorization of 387 by finding all positive Divisors of 387 !
27. The Greatest Common Divisor (GCD) of integers a and b is the largest positive Divisors of integers a and b and The Least Common Multiple (LCM) of integers a and b is the smallest positive integers that are divisible by integers a and b. If $a = p_1^{m_1} \times p_2^{m_2} \times \dots \times p_{k-1}^{m_{k-1}} \times p_k^{m_k}$ and $b = p_1^{n_1} \times p_2^{n_2} \times \dots \times p_{k-1}^{m_{k-1}} \times p_k^{n_k}$, where p_i are prime numbers, m_i are exponents corresponding to prime number p_i in the factorizations of integer a, n_i are exponents corresponding to prime number p_i in the factorization of integer b, and k denotes the total number of distinct primes that are involved in the factorizations of both a and b, express the Greatest Common Divisor and the Least Common Multiple in terms of p_i, m_i, and n_i !

MODULAR ARITHMETIC

- Kelvin Asclepius Minor –

28. The Euclidean Algorithm is an efficient method for finding the Greatest Common Divisor of integers a and b by applying Division Theorem $b = a \times q + r$. The algorithm computes integers q and r, then replaces b with a and a with r which requires computing new integers q and r. The algorithm repeats the process until $r = 0$ and the non-zero remainder from the last division before reaching zero is the Greatest Common Divisor. Find the Greatest Common Divisor of 48 and 18 !
29. Find the Greatest Common Divisor of 105 and 189 !
30. Find the Greatest Common Divisor of 56 and 15 !
31. Find the expression for the multiplication of Greatest Common Divisor and the Least Common Divisor !
32. Find the Least Common Divisor of 48 and 18 using the multiplication of Greatest Common Divisor and the Least Common Divisor !
33. Bézout's Theorem states that for any two integers a and b, there exist integers x and y such that $GCD(a, b) = ax + by$ that can be expressed as a Linear Combination of a and b. Show that the Greatest Common Divisor of 48 and 18 is the Linear Combination of 48 and 18 !
34. Show that the Greatest Common Divisor of 105 and 189 is the Linear Combination of 105 and 189 !
35. Show that the Greatest Common Divisor of 56 and 15 is the Linear Combination of 56 and 15 !
36. The Multiplicative Inverse of integer b modulo a can be obtained using the Linear Combination if the Greatest Common Divisor of a and b is definitely 1, and if this is not the case, the inverse does not exist. Find the Multiplicative Inverse of 3 modulo 13 !
37. Find the Multiplicative Inverse of 11 modulo 15 !
38. In the Division Theorem, given 3 integers a, b, and c, if $a|b$ then $a|(bc)$. If $r \equiv b\ (mod\ a)$, then what is the congruence of cr modulo a ?
39. Find the solution of $3x \equiv 4\ (mod\ 13)$!
40. Find the solution of $11x \equiv 3\ (mod\ 15)$!

MODULAR ARITHMETIC

- Kelvin Asclepius Minor –

41. The set of equivalence classes $\mathbb{Z}_a = \{0, 1, 2, 3, \dots, a-1\}$ can be considered as a Group of Addition if it satisfies Closure property which ensures that combining any two elements in the group yields another element in the same group, Associativity property which ensures that the way of addition does not affect the outcome, has Identity element that acts as a neutral element, meaning it leaves other elements unchanged when combined with any element, and has Inverse element that acts as a counterpart element under the group operation, meaning it produces the Identity element when combined with any element. Show that $\mathbb{Z}_5$ is a Group of Addition modulo 5 !
42. Show that $\mathbb{Z}_5$ is a Group of Multiplication modulo 5 !
43. Show that $\mathbb{Z}_5$ is a Group of Multiplication modulo 5 by excluding number 0 !
44. Show that $\mathbb{Z}_6$ is a Group of Addition modulo 6 !
45. Show that $\mathbb{Z}_6$ is a Group of Multiplication modulo 6 !
46. For the set $\{1, 2, 3, \dots, a-1\}$ modulo a, what kind of number of a that can be considered as a Group of Addition & Group of Multiplication ?
47. If $\{1, 2, 3, \dots, a-1\}$ is a Group of Multiplication modulo a and k is not divisible by a, then determine the result of $k \times 2k \times 3k \times \dots \times (a-1)k \ mod(a)$!
48. If $\{1, 2, 3, \dots, a-1\}$ is a Group of Multiplication modulo a and k is not divisible by a, then verify the Fermat's Little Theorem by identifying the congruence of k^{a-1} modulo a !
49. Calculate 3^{14} $(mod\ 5)$!
50. Calculate 6^{54} $(mod\ 11)$!