Lesson Review: Module Summary

Response to and Request for feedback

If you are resubmitting, include a statement outlining the changes you have made to your submission. This section can be short but should be precise. It is a good idea to quote the feedback you are responding to.

If this is your first submission, include a statement about what part of the lesson review you would most like to receive feedback (and why). Your tutor will take this in consideration when reviewing your work, although they may choose to give you feedback on a different thing if they think it's more appropriate.

Module Learning Objectives

I certify that I achieved the following learning objectives for the module (these objectives can be found in the introduction of the module):

1. . Compute the prime factorisation of integers and use it to compute the lowest common multiple and greatest common divisor of two numbers.
2. Apply the Euclidean algorithm for finding the greatest common divisor of two numbers.
3. Convert between number bases representations of numbers.
4. Compute the values of large powers of a number in modular arithmetics.

Summarising the content:

- Identify the key terms and concepts in the module. For each of these terms and concepts:
  - Define the term and explain the concept **in your own words** (beware plagiarism – this is an assessment task).
  - Summarise the most important results related to these concepts, including theorems and propositions, algorithms and procedures, etc.
  - You can provide examples, figures, diagrams, but only if they help illustrate your point. This is a summary, so it's best to restrict the explanations to the main points.
  - Make sure you include references to the Module Learning Objectives.

Integers, Factors, and Primes

Division of Integers

If a and b are integers, with $a \neq 0$, a divides b if there is an integer k such that $b = ak$.\

This is denoted by $a|b$.

For example: 3 **|** 12 means "3 divides 12", which is true since 12 = 3 × 4. If a does not divide b, however, this is written as $a \nmid b$, e.g. $5 \nmid 7$.

Division of Integers: Corollaries

Factor and Multiple: If $a \mid b$, we say that a is a factor of b, b is a multiple of a.

Properties of division

We can use this definition to prove the following:

Given three integers a, b and c:

1. $a \mid a$ for all a (a is always a factor of itself).

2. $1 \mid a$ for all a. (a is always a multiple of 1).

3. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$. (if a is a factor of b and of c, then, a is a factor of their sum $b + c$).

4. If $a \mid b$, then for any c,$a \mid bc$ (if a is a factor of b, then a is a factor of b multiplied by any number c).

5. If $a \mid b$ and $b \mid c$, then $a \mid c$ (if a is a factor of b and b is a factor of c, then a is a factor of c).

Prime Numbers and composite numbers:

A positive integer $p > 1$ is:

- prime if it is only divisible by itself and 1;
- composite if it has other positive factors other than itself and 1

Prime Factorisation

To find factors of a number n, successively divide the number by primes in descending order from the one closest to but smaller than √n.

For example: Factorising 60.

To find the prime factorisation of 60:

we have 7 ≤ √60 < 11 (because 7 2 = 49 < 60 < 112 = 121).

The prime numbers to try are {2,3,5,7}.

- $7 \nmid 60$; • $60 = 5 \times 12$, and $5 \nmid 12$;
- $12 = 3 \times 4$, and $3 \nmid 4$;
- $4 = 2 \times 2$ and $2 = 2 \times 1$, and $2 \nmid 1$

. So, $60 = 5 \times 3 \times 2 \times 2$.

GCD and LCM Greatest Common Divisor (GCD) and Least Common Multiple (LCM)

Greatest Common Divisor: The greatest common divisor of a and b, denoted gcd(a,b) is the largest integer d such that $d \mid a$ and $d \mid b$.

Least Common Multiple: The least common multiple of a and b, denoted lcm(a,b) is the smallest positive integer k such that $a \mid k$ and $b \mid k$.

Both the gcd and the lcm can be easily found when a and b are represented by their prime factorisation

Method (Finding the GCD and the LCM)

Take two numbers represented by their prime factorisation

- To find their gcd, take each prime factor the minimum number of times it appears in each of the factorisation
- To find their lcm, take each prime factor the maximum number of times it appears in each of the factorisation

For example:

Find the GCD of $3^2 \times 5 \times 7^4$ and $2^3 \times 3 \times 5^3$.

gcd $3^2 \times 5 \times 7^4$ and $2^3 \times 3 \times 5^3$

= gcd($2^0 \times 3^2 \times 5^1 \times 7^4$,$2^3 \times 3^1 \times 5^3 \times 7^0$)

= $2^0 \times 3^1 \times 5^1 \times 7^0 = 3 \times 5$

For example Find the LCM of $3^2 \times 5 \times 7^4$ and $2^3 \times 3 \times 5^3$.

Lcm $3^2 \times 5 \times 7^4$ and $2^3 \times 3 \times 5^3$.

= 23 × 32 × 53 × 74 .

Euclidean Algorithm: Introduction

Calculating the GCD by first finding the prime factors of the given numbers is computationally expensive. The Euclidean Algorithm is a much faster process.

Consider two integers a and b, where $b > a$. The Euclidean Algorithm makes use of the fact that we can relate the two numbers as follows

$b = m \times a + r0$

i.e. when we divide b by a, we get a multiplier m and a remainder $r0$ It turns out that gcd(b,a) = gcd(a,$r0$).

Numeral Systems

Base Conversion

n Our numeral system is a Base 10 system, i.e. the digits are in consecutive ascending powers of 10 from right to left. For example, the number 837 is $8 \times 10^2 + 3 \times 10^1 + 7 \times 10^0$.

However, bases other than 10 are used.

For example: Computers use base 2 (binary), base 8 (octal), and base 16 (hexadecimal).

Modular Arithmetic

Introduction to Modular Arithmetic

If an integer a, when divided by another integer m, has a remainder $r \geq 0$, then we can write

$r = a \bmod m$.

Which is equivalent to

$a = km + r,\ k \in \mathbb{Z}$.

For example:

17 mod 2 = 1 (as 17 = 8 × 2 + 1)

17 mod 7 = 3 (as 17 = 2 × 7 + 3)

17 mod 9 = 8 (as 17 = 1 × 9 + 8)

Negative Numbers

For a negative integer$a$, a mod m can be found by adding a multiple of m to a to obtain a positive number.

For example:

−108 mod 13 = (−108 + 117) mod 13 = 9

−253 mod 29 = (−253 + 261) mod 29 = 8

Reflecting on the content:

- What is the most important thing you learnt in this module?

  The most important thing I learned in this module is the foundational concepts of integer division, prime factorization, GCD, LCM, Euclidean Algorithm, numeral systems, modular arithmetic, and handling negative numbers in the context of mathematics.

- How does this relate to what you already know?

  This module relates to what I already know by expanding my understanding of fundamental mathematical concepts and providing me with practical methods for solving problems involving integers, factors, primes, and arithmetic operations.

- Why do you think your course team wants you to learn the content of this module for your degree?

  I believe my course team wants me to learn the content of this module for my degree because it forms the basis for more advanced topics in mathematics and various other disciplines. Understanding these concepts is crucial for developing problem-solving skills, logical reasoning, and the ability to analyze and interpret data. Additionally, proficiency in these areas is often required for further studies in fields such as computer science, engineering, physics, and economics.