Name: abdelkareem soubar/19110022
Assessor:Eng. Moath Sulaiman
Course Number and Title: 30202180   Maths for Computing

1.

Division Table

5	5	13
13	1	13
1	1	

LCM = 5 x 13
LCM = 65
LCM(5, 13) = 65

2. Division Table

2	84	112
2	42	56
2	21	28
2	21	14
3	21	7
7	7	7
1	1	

LCM = 2 x 2 x 2 x 2 x 3 x 7
LCM = 336
LCM(84, 112) = 336 months

3.

Definition

An integer x is the modular multiplicative inverse of an integer an if ax is congruent to 1modular some modulus m. To put it another way, we're looking for an integer x such that

a·x≡1modm.
x will also be denoted by the letter a1.

It's worth noting that the modular inverse isn't always present. Consider the case where m=4 and a=2. It should become cl by verifying all possible values modulo It is evident that a1 does not satisfy the preceding equation. The modular inverse may be demonstrated to exist if and only if a and m are relatively prime (i.e. gcd(a,m)=1).
Another way to find the modular inverse is to use theorem, which states that if a and m are relatively prime numbers, the following congruences are true: a (m) ≡1modmϕ is Euler Totient function. Note again that a and m are relatively prime numbers and are conditions for the existence of modular inverses. If m is a prime number, this simplifies to Fermat little theorem: am-1≡1modm Multiplying both sides of the above equation by a-1, we get: For any (but relatively prime) modulus m: a (m) −1≡a -1modm for the prime modulus m: am-2≡a-1modm From these results, we can easily find the modulo inverse using the binary exponentiation algorithm, which works in O time (logm). Although this method is easier to understand than the method described in the previous paragraph, if m is not a prime number, we need to calculate Euler function, which involves factoring m, which can be very difficult. If the prime factorization of m is known, the complexity of this method is O (logm).
Although this method is easier to understand than the method described in the previous paragraph, when m is not a prime number, we need to calculate the Euler phi function, which involves the decomposition of m, which may be very difficult. If the prime factorization of m is known, the complexity of this method is O (logm).

The problem is as follows:
We want to calculate the modular inverse of each number in the range [1, m-1]. Applying the algorithms described, we can obtain a solution with a complexity of O (mlogm). Propose a better algorithm with a complexity of O(m). However, for this particular algorithm, we require the modulus m to be prime. We use inv [i] to denote the modular inverse of i. Therefore, for i> 1, the following equation is valid: inv [i] =-⌊mi⌋·inv [mmodi] modm
1(MOD M)

9 MOD 8 = 1
18 MOD 8 =2
27 MOD8 = 3

$$\sqrt[8]{25}=1$$

$$\frac{1}{9\,MOD\,8}=1 \qquad \frac{1}{18\,MOD\,8}=0.5 \qquad \frac{1}{27\,MOD\,8}=\frac{1}{3}=0.333333$$

4. a) s = $\frac{a_n+1}{a_n}$

$$\frac{4.9}{5} = 0.98 \quad \frac{4.802}{4.9} = 0.98 \quad \frac{4.70596}{4.802} = 0.98$$

s = 0.98
a(1) = 5

$$a_n = a_1 * s^{n-1}$$

method (2) for a)

$$a_1 \frac{1-r^n}{1-r}$$

$$5\frac{1-0.98^{10}}{1-0.98}$$

=0.45.73179

b)
6-3=3
9-6=3
2-9=3
d=3
a_1=3
a_n=a_1+(n-1)d
a_n=3(n-1)+3
day 90
=3(90-1)+3
=270
270+102400
=102670 KB

5.

40%female
85% inattention
15% else

60% male
30% exceeding speed limit
70%else

(40/100)*85= 34%

6.

2%^5
=3.2*10^-9

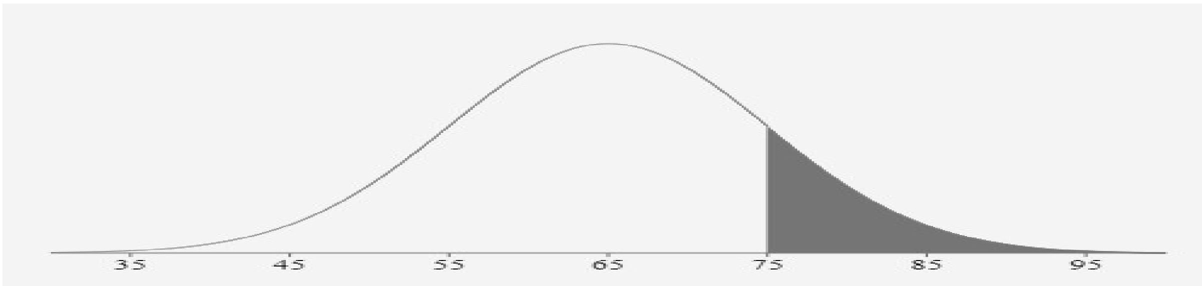
7. A)
3/6 = 0.5
0.5^5
=0.03125*100
=3.125%
B)
3/6 = 0.5
0.5^8

$= \frac{1}{256}$

C)
1-(the normal probability)
1-(0.5^8)

$=1-\frac{1}{256}=0.99609375\%$

8. a)



$$p=(75<x<100)=p(75-65<x<100-65)=p(\frac{75-65}{10}<\frac{x-u}{\partial}<\frac{100-65}{10})$$

$$z=(\frac{x-u}{\partial}<\frac{75-65}{10})=1,\frac{100-65}{10}=3.5$$

$$p(1<z<3.5=0.1585*5000=793)$$

b)

$$(3.5=\frac{\partial-65}{10})$$

$$(0.55=0.13=\frac{7-65}{10}=63.7)$$

9.

1. Introduction

Any integer greater than 1 is classified as a prime or composite number. This classification forms the basis of number theory as we know it today. This article attempts to outline prime numbers, their properties, and their importance in various research fields. It also attempts to clarify some attempts to find the prime of a number, that is, to check whether a given number is prime. Various algorithms have been introduced in history, but none of them has satisfactory speed or efficiency. In fact, the great difficulty involved in finding the prime number of a number and its special properties is precisely the reason why prime numbers are so widely used in the world today. Definition of prime number Definition 1 (English): A prime number (or prime number) is a natural number, which happens to have two different natural numbers. Divisor Definition

2 (Mathematics):

A natural number greater than 1 is a prime number (or a prime number) if the following conditions are met: $\forall$ b $\in$ N b | a $\Rightarrow$ b = 1 $\vee$ b = a.

(1) On the contrary, a composite number can be defined as a natural number, which can be expressed as the product of two natural numbers, neither of which is itself. According to the above definition, 1 is not considered a prime or composite number. In addition, the discussion of prime numbers and composite numbers is limited to positive integers. The importance of prime numbers

3.1 Number theory Any integer greater than 1 is a prime number or a product of prime numbers. This can be easily displayed by summarizing all integers. This means that we can define any integer greater than 1 as the product of one or more elements in the set of all prime numbers. Conversely, combinations of prime numbers can be multiplied to produce any number.

3.2 Cryptography 3.2.1) The RSA system in cryptography uses prime numbers in a broad way to calculate public and private keys. The strength of the system is based on the difficulty of factoring large numbers, particularly the difficulty associated with finding specific selected pairs of prime numbers to create large integers called moduli. 3.2.2)

The Diffie-Hellman key exchange in cryptography uses prime numbers in a similar way. It uses a large prime number p as a public module. Based on this module, two entities, such as A and B, can communicate securely using their undisclosed private keys. Mainly based on this nature, if A and B both choose a private key, they say'a' and'b' respectively, and agree on a number, such as'g' public, where'g' is less than'p' , Then both A and B can send messages to the other, as follows: Message from A = M1 = ga modulo p Message from B = M2 = gb modulo p Then, X = M2a modulo p = M1b modulo p = g (a * b) Module pIs share messages. Its security is that it is difficult to find shared messages without knowing any private key. 3.3 Gödel number Gödel number is a function, which assigns a unique natural number to each expression, called Gödel number. The creator, Kurt Gödel, uses prime numbers to encode all the numbers in the sequence. Since prime numbers have no subprime factors, each expression can only have one Gödel number, which eliminates the ambiguity. In addition, each Gödel number can only be assigned to one expression. In addition, we can use this function to determine whether a given number is a Gödel number. 3.4 Computer Science: Hash Code Calculation A hash code is the digital code of each object created by the program. The hash code is necessary to quickly retrieve/store complex objects from/in the hash table. The hash code of each object must be reasonably unique in order to maintain correctness. For this reason, prime numbers are used to calculate hash codes. For example, Java calculates the hash code of a string as follows: s [0] * 31 (n-1) + s [1] * 31 (n- 2) +… + s [n-1] * 310 where's' is A string consisting of'n' characters, numbered 0-n-1, s [x] represents the ASCII value of the xth character in s. The number 31 is a prime number close to a power of 2 (it is actually a Mersenne prime number, as we will see later). Prime numbers are chosen because they can better distribute data across hash buckets. Since they have no other factors other than themselves and 1, so if x is a prime number, the function of "modulo x" is guaranteed to produce a wider response, if x is not a prime number, it can guarantee a wider response, thus Increase the number of hash cubes.

10. Many activities of a computer system can be summarized in such a way that dividing objects into groups and assigning objects to groups is as balanced as possible. A classic example is a dictionary data structure where "items" refer to "groups" of key/value pairs and stores. Another example is a distributed key-value store. Here container refers to disk space or total server space. A third example could be a distributed runtime engine. In this case, they represent processes, container enumerations, devices, etc. A common approach is to use a hash function that extracts the elements into a relatively short fixed-length string. A hash function is used to somehow associate an item with a bucket. Using a hash function is usually the first step in a solution and requires additional algorithmic considerations to resolve hash value collisions and

inconsistencies. This study describes some of these techniques. Elements are grouped using multiple independent hash functions that focus on a multi-select scheme, which is typically placed in the least loaded bucket when the element is placed. We take a closer look at the resulting distribution and show you how to use these ideas to design underlying data structures. Focus on dictionaries, linear searches, cuckoo partitions, and more. It is based on data structures.

"Load balancing" is an umbrella term for various algorithmic problems that require groups of sets of elements to be defined, although the load in each group is distributed almost equally. Load balancing in this general way is one of the most basic and common problems with algorithms. Typical applications include hard drives and storage systems where block files or objects are stored, data structures with storage, and distributed engines or switch objects including servers and object containers. This study presents the idea of a number of underlying algorithms that represent interesting practical and theoretical approaches to this problem. The main component is a hash function that specifies the range of elements in a group. Hash functions are actually considered "random" because they are sampled from some family. For example, if the hash function is uniformly sampled as a group from the set of all possible element assignments, then each element is actually assigned to the same sample container, and each element's assignment is independent of the others. In this case, the number of elements assigned to the pair is:
The maximum load distribution and stress can be understood through a relatively standard analysis of the binomial tail distribution.

The first part of this study focused on a computational method called multivariate. It gets its name from the fact that it uses multiple hash functions. At the top level, if there are multiple hash functions, each element is assigned to several groups so that the algorithm designer can select the elements individually. This independence seems to allow the algorithm to get a better ratio than what is achieved with a hash function. Here are some ideas for the underlying algorithms and basic mathematical tools used to improve the restrictions on the instructions generated by these algorithms. From our point of view, it can be seen that a robust analysis of the following model changes explains the effectiveness of these algorithms in real-world applications. Our starting point is the simple "ball-in-box" model describe the multi-selection technique in detail.
Most important to the reader is familiarity with two powerful testing methods: the multi-layer derivation method and the performance-based feature idea . Both test methods are very powerful and are usually used to replace the original model.
The second part of the study focused on the data structure of dictionaries. A dictionary is a simple, generic data structure that supports insertion, deletion, and retrieval of items. Efficient use of the dictionary relies heavily on the principles of load balancing algorithms, particularly the term "cuckoo hack" its various variations. Finally, let's talk about the linear control dictionary. This isn't usually part of a multiple choice scheme, but it's actually faster.

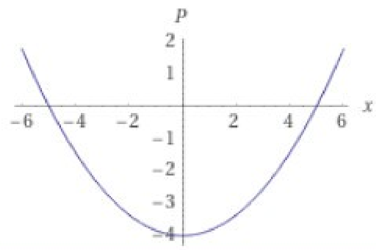
Bullet-in-Box Model: A common framework for thinking about the load balancing process is "bullet" and "box" boxes. The spheres represent requirements (keys, procedures, files, etc.) and boxes represent requirements (keys, procedures). , files, etc.). The "display" character represents a resource (table, table, server, volume, etc.). This studio uses buckets and boxes, objects and balls rather than using each other. The framework does this heuristically by throwing m balls into n boxes. They are usually thrown one by one in turn. The goal is to understand the allocation of balls in the box at the end of the process. It usually contains the container with the greatest load (= number of plies). In this model, nodes are assigned to boxes by one or more hash functions. A property that specifies a unique ball (usually included in the pattern) for a set of boxes (usually the numbers 1 ... n). It's usually convenient to use hashes. Later, when you need to get the ball's position from the ID, you can assign a container to the ball instead of drawing a random basket.

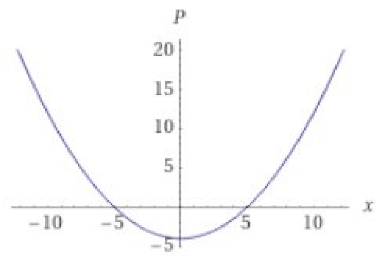
Random Hash Estimation Most studies assume that the hash function used is completely random. This means that h(ball.id) is the same sample container and is independent of h() for all other balls. That is, the family of uniformly sampled functions H are all families of functions in the world for a set of ice frames. It also ignores the time it takes to compute h and the space it takes to store h. This assumption allows you to focus on assignable attributes, providing contextual detail and clear performance. In practice, this hypothesis can be useful when describing algorithms in general, limiting the existence of hash functions and assuming that each element produces the same independent "sample" of the container. In practice, a specific hash function needs to be performed, taking into account the potential properties of the hash function as well as the space required to store it and the time required for computation. It is easy to see that a fully random hash function can be implemented very cheaply in real-world scenarios due to its complexity.

Dictionary data structure algorithms overcome this task. In many cases, much work has been done to break these assumptions and study the desired time/space/condition balance for a particular application. The starting point for this research direction is the pioneering work of Carter and Wegman [24] in the field of global segmentation. This study assumes a random hash.

A dictionary is a data structure that stores key/value pairs and supports additional functions (key/value), delete (key), and search (key). This is one of the oldest and most widely used data structures. It was first widely implemented in the 1950s [46, 92]. Many implementations are found in almost all standard libraries. There are several ways to implement a dictionary considering the algorithm. let's take this as an introduction. The idea is to use a hash function h that puts the domain key into a set [n]. Matrix A is affected by length n. Ideally you should input a key/value pair (k, v) and convert (k, v) to [h(k)]. This is not possible because you can draw multiple keys on an indexed array. This is a phenomenon called hash collision. A simple sequence hash table solves the problem by treating each element of an array as a key pointer to a linked list and interpreting it as all elements assigned to that array list. The insert method inserts (k, v) pairs into the linked list of A[h(k)]. Similarly, the verb (k) finds the key k in the same linked list. There are several ways to list, but in both cases the search time can be equal to the number of elements assigned to each index in the array. For example, the maximum length of a linked list. The length of the coil exactly matches the pattern of the canned balls.

11.





P = 0.16 (x - 5) (x + 5)
P = 0.16 x^2 – 4
x = ± 5
P all real numbers : P>=-4
b)
even, because first off all the plot is the lest side is the same as the right side (it even when when the same number is represented as the same value in the + side and – side and its the equation is squared .
c)
the right side (from0 to ∞) is increasing and (from ∞ to 0) it is decreasing.

12-)
a)
a · b = ax · bx + ay · by + az · bz = 5 · 2 + 3 · 2 + (-3) · 3 = 10 + 6 - 9 = 7
|a| = $\sqrt{ax2+ay2+az^2}$ = $\sqrt{5^2+3^2+-3^2}$ √52 + 32 + (-3)2 = √25 + 9 + 9 = √43
|b| = $\sqrt{bx2+by2+bz^2}$ = $\sqrt{2^2+2^2+3^2}$ = √4 + 4 + 9 = √17
cos α = $\left(\frac{a \cdot b}{|a||b|}\right)$

cos α = $\left(\frac{7}{\sqrt{43}\cdot\sqrt{17}}=\frac{7\sqrt{731}}{731}\right)\approx 0.25890435250935817$

b)
a × b =

i	j	k
ax	ay	az
bx	by	bz

=

i	j	k
5	3	-3
2	2	3

= i (3·3 - (-3)·2) - j (5·3 - (-3)·2) + k (5·2 - 3·2) = i (9 + 6) - j (15 + 6) + k (10 - 6) = {15; -21; 4} c)

v1=5i+3j-3k
2v1=10i+6j-6k
v2=2i+2j+3k
2v2=4i+4j+6k

v1+v2= 7+5+0 = 12*2 =24

2v1+2v2= 14+10+0=24
2v1+2v2 = 2(v1+v2)
(v1 v2)=10 + 6 - 9 = 7

13)
Coordinate System: Think of your computer screen as a "playground" like a soccer ball or soccer ball. Playgrounds are a great analogy when thinking about how computer games display objects on the screen. Move game objects around the screen in the same way that players move around the arena. You can even design your own soccer or soccer match according to your schedule! In computer science, the phases displayed on a computer screen are called coordinate systems. You probably studied the coordinate system by studying logarithmic graphs. However, computer coordinate systems differ from the algebraic coordinate systems you learn in school in two ways. First, I am not claiming to contain an infinite number of points along the x (horizontal) and y (vertical) axes because computer screens are so small and have sharp edges. On the other hand, the number of websites that can be displayed on the screen is limited. Then the y-axis moves down on the computer screen instead of up as in the logarithmic diagram. Because of this difference, computer coordinate systems and logarithmic coordinate systems are not compatible, but they usually use their own coordinate systems because they depend on how TVs and computer monitors have been made over the past 60 years. It's not difficult once you get used to it. In practice, computers use the (x, y) coordinate system where the left edge of the screen is x = 0 and the left edge of the screen is on the screen. is Vertex y = 0 defines that the origin (x = 0 and y = 0) is in the upper left corner of the page. Moving to the right of the screen increases the x value, and moving it down increases the y value. Figure 2.4 shows the program in different positions (x, y). The first value of each pair is the x value for that position on the screen. As you can see, the value of x increases as we move from left to right. The second value is the y value of the position on the screen, increasing as you move up and down. Next, let's take a closer look at the steps in the myUFO program to understand how coordinate systems work. The seventh line contains the expression myUFO.MoveTo(50, 50). Position (x, y) (50, 50) moves the object 50 pixels down on the x-axis and 50 pixels down on the y-axis. As you can see, the distance from the top left corner of the screen is not great. On a computer screen, we don't think much about individual pixels. Everything you see is made up of a large number of pixels or colored dots. The program window will open while the program is running. As shown in Figure 2.4, the height is at least 500 pixels and the height is at least 400 pixels. Also, what happens if you try to reposition the UFO? can help you understand. Click on (50, 50), change it to another value like (300, 50), repeat the program several times, then run the program again. The way the coordinate system works is very important to most of the programs you'll create, especially if you're using a different language than the program itself. So, you should read this section until you understand and try until the last step is the simplest. Tell Frogram where to take a picture via myUFO and where to look, then instruct Frogram to look at the picture on the screen. It's simple:

In the context of coordinate system design, the term is often used as a synonym for coordinate system. To configure or change the projection/coordinate system, see Projection. This topic provides basic information about coordinate systems. When using geospatial data, you need to know your location. A coordinate system is a systematic way of describing a place using numbers. I need that data. All this data imports a lot of spatial data into the coordinate system database it uses. Often all spatial data is stored in a table, and the coordinate system used to interpret the spatial data in the table is defined in the table's properties. There are many ways to describe places using numbers, but an easy way to learn in school is to use two numbers for each place: an X number and a Y number. Use this system to draw a curve on graph paper with an X number to the left or right, a Y number to indicate the distance to the left or right, and a Y number to indicate the difference between the top and bottom points. X and Y Coordinates X and Y values represent coordinates.

Coordinate System Definition/Prediction Describes how computers typically define new coordinate systems and calculate places on Earth before publishing documents that describe equations, parameters, or other tools. It was the target. X, Y, Z are A. The coordinate system is displayed. Its name is a coordinate system like the Lambert cone projection. Storing geospatial data using only text names and defining predictions as they are exchanged does not mean that all of the various choices and settings required for text names will appear. It is causing endless problems. For simplicity, the system must specify exactly the name of the coordinate system and all the options and parameters in addition to the coordinates that must be specified. For example, we have two separate discs, one censoring Ohio's roads and one censoring Ohio's rivers and lakes, and showing only two records. Let's say you don't have enough computers. When asked to use the Lambert Cone matching system, they do so. For example, if you have a road and a river and you cross the road, you can interpret the data correctly in the coordinate system, but you cannot see it from the center of the lake. You must also specify the context or criteria to use, the standard inference to use, and other options and parameters. There are three main features that allow you to distribute and exchange spatial data sets between different users and different applications without much confusion about the coordinate system.

Standard Names: A standard and unique way to name a coordinate system is required. If the Arkansas environment reads the correct coordinate system of the Lambert cone, it takes precedence, which Henry of Hong Kong calls a cone design error. Spatial file format: You need a way to influence a specific data set, with a coordinate system used for all the details you need. You get a number file, but without information about the coordinate system, those numbers are useless for geospatial data. Accurate calculations: The computer programs we use must efficiently and accurately perform all necessary calculations, including transformations between them, to interpret all necessary coordinate systems. None of the above functions are clear. A lot of geospatial data around the world uses anonymous names. The world's most widely used standard for storing geospatial data does not have the ability to assign that coordinate system to a file. The ability to accurately perform system coordinate calculations is noteworthy. Therefore, when working with geospatial data, it is very difficult to understand which coordinate system is used, which parameters are missing, and other budget issues where all three are not required. Basically.. the most advanced systems have geospatial rules to deal with issues like diversity. One of the many ways to make life easier for geospatial users is by identifying almost every other naming system in your coordinate system, or deciding which one to use for a particular data set.

Coordinate System Names World coordinate system names are usually defined in a coordinate system or set of standard prediction systems.
Definitions published by national cartographic organizations
Definitions published by EPSG
Definitions published by other groups: B OGC

National Cartographic Agency The literal names of coordinate systems such as the B. Lambert isometric cone projection are defined relatively equally in each country by national cartographic officials such as the USGS in the United States and the IGN in France. These are often government organizations, but may also be non-governmental organizations. Since GIS was first developed in the United States and the American software industry had a major impact on the world, the names of the scripts used by the USGS can be found in a collection of technical articles written by USGS authors. John Parr Snyder was a big influence here. The whole world names the coordinate system in English. For known coordinate system names, Manifold uses the names and associated definitions from USGS publications. If coordinate systems are used in some countries and the National Mapping Office publishes the names of these coordinate systems, Manifold uses the names provided by that country mapping office. These text names appear in the Long Coordinate System Names list in the World Coordinate System dialog box.

EPSG Code EPSG is a numeric code such as EPSG: 3857 that accurately identifies all algorithms associated with a coordinate system in a database of thousands of EPSGs. EPSG also contains literal names for each symbol. The European Petroleum Survey (EPSG) was a scientific organization of European oil industry experts who developed a standard database of coordination systems and related information to facilitate the technical work of oil and gas exploration. EPSG joined the International Association of Oil and Gas Producers (IOGP) in 2005, but the database is still managed as the EPSG database. EPSG codes are the most complete and confusing way to define a specific coordinate system. EPSG accuracy and technical quality are also the best standard tools for accurate determination and transformation of coordinate systems. Despite the high standards of major national guidance agencies such as the USGS in the United States and IGN in France, the quality of EPSG graphics is simply the best in the world. The EPSG database synchronization system poses a threat to any program because it contains thousands of EPSG codes, but EPSG has become the standard for defining coordinate systems because of its accuracy and integrity. .. EPSG database is free to download. You can specify a coordinate system using EPSG codes on the EPSG tab of the Collector's Coordinate System dialog box. The header supports all EPSG cables, including obsolete cables and cables that have been replaced with other cables. For example, EPSG: 26747 is replaced by EPSG: 26799. Unfortunately, not all applications use EPSG symbols correctly. Some programs claim to use EPSG codes, but ignore important parts of the standard. Check out this YX

STUDENT ASSESSMENT SUBMISSION AND DECLARATION

When submitting evidence for assessment, each student must sign a declaration confirming that the work is their own.

Student name: ABDELKAREEM YOUSEF MAMDOH SOUBAR **Student ID: 19110022** **Is the student repeating this unit? NO**		**Assessor name:** Eng. Moath Sulaiman
Issue date: 17/8/2021	**Submission date:** Sep. 3rd 2021 8:00 PM	**Submitted on: Sep. 3rd 2021**
Program: Computing		
HTU Course Name: Maths for Computing **HTU Course Code:** 30202180		**BTEC Course Title:** Maths for Computing **BTEC Course Code:** D/615/1635
Assignment number and title: Assignment 6: **Euclidia SW**		

Plagiarism

Plagiarism is a particular form of cheating. Plagiarism must be avoided at all costs and students who break the rules, however innocently, may be penalized. It is your responsibility to ensure that you understand **correct referencing practices**. As a university level student, you are expected to use appropriate references throughout and keep carefully detailed notes of all your sources of materials for material you have used in your work, including any material downloaded from the Internet. Please consult the relevant unit lecturer or your course tutor if you need any further advice.

Student declaration

I certify that the assignment submission is entirely my own work and I fully understand the consequences of plagiarism. I understand that making a false declaration is a form of malpractice.

Student signature: **Date: Sep. 3rd 2021**