**STAGE 1 MATHEMATICS**

**ASSESSMENT TYPE 2: MATHEMATICAL INVESTIGATION**

**MATRICES**

**NAME :**

Your report on the mathematical investigation should include the following:

* an outline of the problem and context
* the method required to find a solution, in terms of the mathematical model or strategy used
* the application of the mathematical model or strategy, including:
	+ relevant data and/or information
	+ mathematical calculations and results, using appropriate representations
	+ the analysis and interpretation of results, including consideration of the reasonableness and limitations of the results
* the results and conclusions in the context of the problem
* a bibliography and appendices, as appropriate.

The format of an investigation report may be written or multimodal.

The investigation report should be a **maximum of 8 A4 pages** if written, or the equivalent in multimodal form.

**Assessment Design Criteria**

**Concepts and Techniques**

CT1 Knowledge and understanding of concepts and relationships

CT2 Selection and application of mathematical techniques and algorithms to find solutions to problems in a variety of contexts

CT3 Application of mathematical models

CT4 Use of electronic technology to find solutions to mathematical problems

**Reasoning and Communication**

RC1 Interpretation of mathematical results

RC2 Drawing conclusions from mathematical results, with an understanding of their reasonableness and limitations

RC3 Use of appropriate mathematical notation, representations, and terminology

RC4 Communication of mathematical ideas and reasoning to develop logical arguments

RC5 Development and testing of valid conjectures

**Coding and Decoding using Matrices**

**Part 1**

This part of the investigation will show you by example how to produce a coded message (enciphering) and how to decode a message (deciphering).

The 26 letters of the alphabet are chosen and a value assigned as show below:

Letters: A 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

Value: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 0

Assign numbers to some plain text and then arrange these numbers in column matrices. For example:

 ALGEBRA becomes AL GE BR AA and with code and column matrix form becomes

 $\left[\begin{matrix}1\\12\end{matrix}\right] \left[\begin{matrix}7\\5\end{matrix}\right] \left[\begin{array}{c}2\\18\end{array}\right] \left[\begin{matrix}1\\1\end{matrix}\right]$

To encipher this message or word we need a coding matrix which is a 2x2 matrix with a determinant that is not divisible by 2 or 13.

An example is$\left[\begin{matrix}1&3\\2&1\end{matrix}\right]$. Pre-multiply each column matrix by this 2x2 matrix. For example,

$\left[\begin{matrix}1&3\\2&1\end{matrix}\right]\left[\begin{matrix}1\\12\end{matrix}\right]=\left[\begin{matrix}37\\14\end{matrix}\right]=\left[\begin{matrix}11\\14\end{matrix}\right]\left(mod26\right)$ . AL has been enciphered as KN.

This gives an enciphered message of KNVSDVDC.

To decipher a code with the enciphering matrix known, rewrite the code in number form and produce column matrices. Then with the enciphering matrix, find its determinant and then the reciprocal modulo 26 of that number. For example, consider the enciphering matrix $\left[\begin{matrix}4&1\\3&2\end{matrix}\right]$ which has a determinant of 5. This has a reciprocal modulo 26 value of 21. The following table will help with other values for the determinant:

|  |
| --- |
| Determinant and the reciprocal modulo 26 |
| Determinant | 1 | 3 | 5 | 7 | 9 | 11 | 15 | 17 | 19 | 21 | 23 | 25 |
| Reciprocal modulo 26 | 1 | 9 | 21 | 15 | 3 | 19 | 7 | 23 | 11 | 5 | 17 | 25 |

Now convert the enciphering matrix to a deciphering matrix:

$\left[\begin{matrix}4&1\\3&2\end{matrix}\right]^{-1}=21\left[\begin{matrix}2&-1\\-3&4\end{matrix}\right]=\left[\begin{matrix}16&5\\15&6\end{matrix}\right] (mod26)$

Use this deciphering matrix to pre-multiply coded column matrices and hence decode the message.

**Part 2 – Coding and Decoding**

Encipher your own message using Part 1 and give it to another member of the class along with your enciphering matrix. In return obtain their coded message, enciphering matrix and decode their message.

Consider and discuss any limitations with this method of encryption.

**Part 3 – Further Considerations**

Below is a list of suggestions for further consideration within the scope of this investigation.

* Consider Part 1: Why is it necessary when using modulo 26 to have a determinant which is not a factor of 26?
	+ An investigation into relevant modulo arithmetic
	+ Production of a calculator program or computer program to find reciprocal modulo numbers.
* Consider how larger amounts of text may be coded/decoded rather than two letters at a time.
* Consider allowing the use of punctuation.

Performance Standards for Stage 1 Mathematics

|  |  |  |
| --- | --- | --- |
|  | **Concepts and Techniques** | **Reasoning and Communication** |
| **A** | Comprehensive knowledge and understanding of concepts and relationships.Highly effective selection and application of mathematical techniques and algorithms to find efficient and accurate solutions to routine and complex problems in a variety of contexts. Successful development and application of mathematical models to find concise and accurate solutions.Appropriate and effective use of electronic technology to find accurate solutions to routine and complex problems. | Comprehensive interpretation of mathematical results in the context of the problem.Drawing logical conclusions from mathematical results, with a comprehensive understanding of their reasonableness and limitations.Proficient and accurate use of appropriate mathematical notation, representations, and terminology.Highly effective communication of mathematical ideas and reasoning to develop logical and concise arguments.Effective development and testing of valid conjectures. |
| **B** | Some depth of knowledge and understanding of concepts and relationships.Mostly effective selection and application of mathematical techniques and algorithms to find mostly accurate solutions to routine and some complex problems in a variety of contexts.Some development and successful application of mathematical models to find mostly accurate solutions.Mostly appropriate and effective use of electronic technology to find mostly accurate solutions to routine and some complex problems. | Mostly appropriate interpretation of mathematical results in the context of the problem.Drawing mostly logical conclusions from mathematical results, with some depth of understanding of their reasonableness and limitations.Mostly accurate use of appropriate mathematical notation, representations, and terminology.Mostly effective communication of mathematical ideas and reasoning to develop mostly logical arguments. Mostly effective development and testing of valid conjectures.  |
| **C** | Generally competent knowledge and understanding of concepts and relationships.Generally effective selection and application of mathematical techniques and algorithms to find mostly accurate solutions to routine problems in a variety of contexts.Successful application of mathematical models to find generally accurate solutions.Generally appropriate and effective use of electronic technology to find mostly accurate solutions to routine problems. | Generally appropriate interpretation of mathematical results in the context of the problem. Drawing some logical conclusions from mathematical results, with some understanding of their reasonableness and limitations. Generally appropriate use of mathematical notation, representations, and terminology, with reasonable accuracy.Generally effective communication of mathematical ideas and reasoning to develop some logical arguments. Development and testing of generally valid conjectures. |
| **D** | Basic knowledge and some understanding of concepts and relationships.Some selection and application of mathematical techniques and algorithms to find some accurate solutions to routine problems in some contexts.Some application of mathematical models to find some accurate or partially accurate solutions.Some appropriate use of electronic technology to find some accurate solutions to routine problems. | Some interpretation of mathematical results.Drawing some conclusions from mathematical results, with some awareness of their reasonableness or limitations.Some appropriate use of mathematical notation, representations, and terminology, with some accuracy.Some communication of mathematical ideas, with attempted reasoning and/or arguments.Attempted development or testing of a reasonable conjecture. |
| **E** | Limited knowledge or understanding of concepts and relationships.Attempted selection and limited application of mathematical techniques or algorithms, with limited accuracy in solving routine problems.Attempted application of mathematical models, with limited accuracy.Attempted use of electronic technology, with limited accuracy in solving routine problems. | Limited interpretation of mathematical results.Limited understanding of the meaning of mathematical results, their reasonableness or limitations.Limited use of appropriate mathematical notation, representations, or terminology, with limited accuracy.Attempted communication of mathematical ideas, with limited reasoning.Limited attempt to develop or test a conjecture. |