The Open University

Faculty of Science, Technology, Engineering and Mathematics

M303 Further pure mathematics

M303

TMA 01 2025J

Mainly covers Book A *Number theory* **Cut-off date 11 November 2025**

You will find instructions for completing TMAs in the Assessment resources area of the M303 website. Please remind yourself of these instructions before beginning work on each TMA. You can submit each TMA electronically by using the University's online TMA/EMA service or by post together with completed TMA form (PT3). In both cases the University must receive it by the cut-off dated given above unless you have agreed an extension in advance with your tutor.

Half of each TMA is formative and the other half summative. The formative questions are designed to *extend* your understanding of the topics, while the summative ones place more emphasis on *assessing* your understanding of the topics. Both types of question will be marked by your tutor, but (unlike the summative questions) marks for the formative questions do not count towards your final grade. You should submit your solutions to both sets of questions to your tutor by the cut-off date.

The marks allocated to each part of a question are indicated in the margin.

Although many of the questions on these assignments require numerical answers, the questions invariably carry *method marks*.

The words listed below, when used in questions, should be interpreted as indicated.

prove, show, explain, justify	Clear reasoning and explanation for all steps are called for.
determine, find, devise, calculate, compute	An indication of the method used and all working in arriving at an answer should be given.
deduce	Clear explanation of how one result follows from another is required.
solve	Working must be shown. A numerical answer alone is not sufficient.
evaluate, give, write down, list	Answer suffices. No explanation need be given.
hence	No marks will be awarded for any alternative method.

PLAGIARISM WARNING – the use of assessment help services and websites

The **work that you submit for any assessment/examination on any module should be your own**. Submitting work produced by or with another person, or a web service or an automated system, **as if it is your own** is cheating. It is **strictly forbidden** by the University.

You should not:

- provide any assessment question to a website, online service, social media platform or any individual or organisation, as this is an infringement of copyright
- request answers or solutions to an assessment question on any website, via an online service or social media platform, or from any individual or organisation
- use an automated system (other than one prescribed by the module) to obtain answers or solutions to an assessment question and submit the output as your own work
- discuss examination questions with any other person, including your tutor.

The University actively monitors websites, online services and social media platforms for answers and solutions to assessment questions, and for assessment questions posted by students. Work submitted by students for assessment is also monitored for plagiarism.

A student who is found to have posted a question or answer to a website, online service or social media platform and/or to have used any resulting, or otherwise obtained, output as if it is their own work has committed a disciplinary offence under our Code of Practice for Student Discipline. **This means the academic reputation and integrity of the University has been undermined.**

The Open University's Academic Conduct Policy defines plagiarism in part as:

- using text obtained from assignment writing sites, organisations or private individuals
- obtaining work from other sources and submitting it as your own.

If it is found that you have used the services of a website, online service or social media platform, or that you have otherwise obtained the work you submit from another person, this is considered serious academic misconduct and you will be referred to the Central Disciplinary Committee for investigation.

This TMA is based on Book A (Number theory), except for the formative Question 9, which covers the start of Book B.

Part A is **summative**. These questions assess your knowledge of the module. You must not discuss these questions in the forums, and your tutor is not allowed to help you directly with these questions.

Part B is **formative**. You should choose (at most) two formative questions to submit to your tutor for marking.

Answering the formative questions will help you to understand key concepts covered in the text. You are encouraged to discuss these questions in the module forums and with your tutor (who is allowed to help you with these questions).

Question 9 is designed to help you with TMA 02. Questions 10 and 11 cover material that is more central to the module, while Question 12 is designed to expand your understanding beyond the core material. In particular, Question 11 introduces ideas that will play a significant role in Books C and E.

Your tutor will mark all the summative answers that you submit and the first two of any formative answers that you submit. If you have attempted at least one formative question then when your TMA is returned you will be sent worked solutions to all the formative questions. Note that only your marks for Part A count towards your overall continuous assessment score.

Part A Summative

Question 1 – 3 marks

This M303 question tests your understanding of material relating to Book A. It uses concepts that you should have covered before starting M303. If you need a refresher on this material then there is a refresher section at the end of the first week on the module planner. Section 6 of the Quick reference section of the Handbook gives the relevant definitions.

(a) Let

$$A = \{1, 2, 3, 4, 5\},\ B = \{\text{cat}, \text{dog}, \text{rabbit}, \text{hamster}\},\ C = \mathbb{Z}\ \text{ and } D = \{\alpha, \beta, \gamma,\ \delta\}.$$

Let $f\colon A \to B$ be defined by

$$f(1) = \text{cat},\ f(2) = \text{hamster},\ f(3) = \text{dog},\ f(4) = \text{rabbit},\ f(5) = \text{cat}.$$

Let $g\colon A \to D$ be defined by

$$g(1) = \alpha,\ g(2) = \delta,\ g(3) = \beta,\ g(4) = \beta,\ g(5) = \alpha.$$

Let $F\colon A \to C$ be defined by

$$F(a) = 100 \times a \text{ for all } a \in A.$$

Let $\phi\colon B \to D$ be defined by

$$\phi(\text{cat}) = \alpha,\ \phi(\text{dog}) = \gamma,\ \phi(\text{rabbit}) = \beta,\ \phi(\text{hamster}) = \delta.$$

Which, if any, of the maps defined above is

(i) a bijection (ie one-one and onto)?

(ii) onto but not one-one?

(iii) one-one but not onto?

(iv) neither one-one nor onto?

[*2*]

(b) Let

$$S = \{2, 3, 5, 7\}$$

and

$$T = \{1, 3, 5, 7\}.$$

(i) Write down a map from S to T that is not one-one.

(ii) Write down a map from S to T that is a bijection.
(Remember that you do not need to provide any explanation or proof to get full marks if a questions says 'write down'.)

[*1*]

Question 2 – 4 marks

This M303 question tests your understanding of material from Chapter 1.

Use mathematical induction to prove that for all integers $n \geq 1$, $7^{2n} - 6^n$ is divisible by 43. [*4*]

Question 3 – 4 marks

This M303 question tests your understanding of material from Chapter 1.

Use the Euclidean Algorithm to determine one pair of integers x and y such that *[4]*

$$\text{hcf}(2025, 630) = 2025x + 630y.$$

Question 4 – 11 marks

This M303 question tests your understanding of material from Chapter 2.

For each of the following statements, decide whether it is true or false. If true, prove it; if false, give a counterexample.

(a) If a and b are positive integers and p is prime, then p divides $\text{hcf}(a^2, b)$ if, and only if, p divides $\text{hcf}(a, b^2)$. *[3]*

(b) If a and b are positive integers and m and n are defined by

$$m = 3a + b \text{ and } n = 5a + 2b$$

then $\text{hcf}(m, n) = \text{hcf}(a, b)$. *[3]*

(c) A number of the form $14a + 3$, where a is a non-negative integer, must have a prime divisor of this same form $14b + 3$, where b is a non-negative integer. *[2]*

(d) If n is divisible by 15 but not divisible by 9 or 25, then $\tau(n)$ is divisible by 4. *[3]*

Question 5 – 8 marks

This M303 question tests your understanding of material from Chapter 3.

(a) Solve each of the following linear congruences (clearly showing your workings).

(i) $3x \equiv 4 \pmod{5}$

(ii) $3x - 1 \equiv 2(4 + x) \pmod{7}$

(iii) $2(7 - x) \equiv 8 - x \pmod{17}$ *[5]*

(b) Determine the least positive integer that satisfies all three of the congruences in part (a). *[3]*

Question 6 – 7 marks

This M303 question tests your understanding of material from Chapter 4.

(a) Use Fermat's Little Theorem to find the least positive residue of $25^{60} \pmod{59}$. *[3]*

(b) Prove that $a^{25} \equiv a \pmod{195}$ for every integer a.

(Note that $195 = 3 \cdot 5 \cdot 13$.) *[4]*

Question 7 – 10 marks

This question tests your understanding of material from Chapter 4.

Throughout this question, let

$$P(x) = x^3 + 23x^2 + 10x + 6.$$

(a) Considering $P(x)$ as a polynomial over the integers modulo 63, state the degree of P. [*1*]

(b) (i) Find all solutions of the polynomial congruence

$$P(x) \equiv 0 \pmod{3}.$$

(ii) Find all solutions of the polynomial congruence

$$P(x) \equiv 0 \pmod{7}.$$ [*5*]

(c) Use the results of part (b) to find all solutions of the polynomial congruence

$$P(x) \equiv 0 \pmod{63}.$$ [*4*]

Question 8 – 3 marks

An important part of being a mathematician is being able to communicate your ideas and thoughts successfully to other mathematicians. In order to help you to develop this skill over the course of the module, each TMA will contain a short question relating to this theme – you are not required to give long answers.

To start you off, we would like you to do the following.

(a) Watch the informal online session entitled 'M303: Things you need to know' that is linked to from Week 1 on the module website. To get the mark for this question you should write in your TMA that you have watched the session. [*1*]

(b) Post something in an M303 module forum. To earn full marks, provide either a screenshot of your forum post or directions as to where to find it (giving the forum where posted, thread title, time and date). (If you are not in a position to provide such evidence, contact your tutor for advice.) [*2*]

Part B Formative

Question 9 – 14 marks

This question concerns material from Book B, and relates to Question 2 in TMA 02.

Let G be the set given by $G = \{a + b\sqrt{-7} : a, b \in \mathbb{Z}\}$. Let $+_G$ be the binary operation on G given by

$$(a + b\sqrt{-7}) +_G (a' + b'\sqrt{-7}) = (a + a') + (b + b')\sqrt{-7},$$

for $a, a', b, b' \in \mathbb{Z}$.

Let $H = \{a + b\sqrt{-7} : a, b \in 2\mathbb{Z}\}$ (where $2\mathbb{Z} = \{2n : n \in \mathbb{Z}\}$ is the set of multiples of 2).

(a) Write down the following.

(i) The identity element of $(G, +_G)$.

(ii) An element of H that is not the identity.

(iii) An element of G that is not in H.

(iv) The sum (under $+_G$) of your answers to parts (a)(ii) and (a)(iii). [*2*]

(b) Show that $(G, +_G)$ is a group. [*4*]

(c) By using the subgroup criterion (in additive form, proposition 2.5), or otherwise, show that H is a subgroup of $(G, +_G)$. [*3*]

(d) Explain why H is a normal subgroup of $(G, +_G)$. [*1*]

(e) Write down the order of the element $1 + H \in G/H$. [*1*]

(f) Write down the other three elements of the quotient group G/H, and construct the Cayley table for G/H. [*2*]

(g) Is G/H cyclic? [*1*]

Question 10 – 10 marks

This is a famous puzzle. You can find the solution by searching the internet but you will gain the most from it if you attempt to solve it yourself.

On a rocky planetoid, there are k aliens (where $k \geq 1$) who have blue ears, and the rest of the aliens have green ears. At the start of the puzzle, no alien knows their own ear colour. If an alien discovers that they have blue ears, then they must leave the planetoid at 6 am the following revolution. Each alien on the planetoid knows every other alien's ear colour, but there are no mirrors and there is never any discussion of ear colour, so an alien has no way of determining their own ear colour.

An outsider arrives, calls together all the aliens on the planetoid, and makes the following public announcement: 'At least one of you has blue ears.' The outsider is known by all to be truthful, and all know that all know this. It is common knowledge that the outsider is truthful, so it becomes common knowledge that there is at least one alien with blue ears.

(a) Assuming that all the aliens on the planetoid are completely logical and that this too is common knowledge, what is the eventual outcome and when does it occur? [*2*]

(b) Give a proof that your answer to part (a) is correct. [*8*]

Question 11 – 13 marks

This question introduces ideas that will play a significant role in Books C and E of the module.

For this question you may assume that $\sqrt{p}$ is irrational for all primes p, and that $\sqrt{2}+\sqrt{3}$ is irrational.

A polynomial function with integer coefficients of degree n (where $n \in \mathbb{N}$) is an expression $P(x)$ of the form

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

where $a_i \in \mathbb{Z}$ for each $i = 0, 1, 2, \ldots, n$, and $a_n \neq 0$.

We say that a real number α is a *root* of the polynomial function $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ if $P(\alpha) = 0$ (in other words, if $a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$).

(a) Explain why $\sqrt{2}$, $\sqrt{3}$ and $\sqrt{2}+\sqrt{3}$ are not roots of any polynomial functions with integer coefficients that have degree 1. [*3*]

(b) Let p be a prime number. Write down a polynomial function $P_p(x)$ with integer coefficients that has degree 2 and for which $\sqrt{p}$ is a root. [*1*]

(c) Show that the polynomial function that you found in part (b) cannot be written as the product of two polynomial functions with integer coefficients that both have degree 1. [*5*]

(d) Find a polynomial function with integer coefficients for which $\sqrt{2}+\sqrt{3}$ is a root. What is the degree of your polynomial function? [*4*]

Question 12 – 13 marks

This question involves many concepts from throughout Book A, and asks you to investigate congruences with composite moduli.

Let p and q be distinct odd primes.

(a) Prove that an integer x satisfies $x^2 \equiv 1 \pmod{pq}$ if, and only if, x satisfies both

$$x^2 \equiv 1 \pmod{p} \quad \text{and} \quad x^2 \equiv 1 \pmod{q}.$$ [*2*]

(b) Explain why $x^2 \equiv 1 \pmod{p}$ has exactly two distinct solutions $x \equiv \pm 1 \pmod{p}$. [*2*]

(c) Use the Chinese Remainder Theorem to explain why $x^2 \equiv 1 \pmod{pq}$ has exactly four solutions. [*4*]

(d) Solve the congruence $x^2 \equiv 1 \pmod{95}$. [*3*]

(e) Why does the fact that the congruence in part (d) has four solutions not contradict Lagrange's Theorem in Chapter 4? [*2*]