Manchester Metropolitan University

Department of Computing and Mathematics

Assessment Cover Sheet 2025/26

Module Code and Title	6G5Z0048 Number Theory and Abstract Algebra
Assessment Set By	Killian O'Brien
Assessment ID	1CWK40
Assessment Weighting	40%
Assessment Title	Coursework Assignment
Assessment Type	Report
Hand-In Deadline	see Moodle
Hand-In Format and Mechanism	Submit a single PDF file containing your work

Learning outcomes being assessed:

LO 1: Construct proofs in number theory and group theory.

LO 2: Select and apply appropriate methods to assemble solutions of problems in number theory and group theory.

Note: it is your responsibility to make sure that your work is complete and available for marking by the deadline. Make sure that you have followed the submission instructions carefully, and your work is submitted in the correct format, using the correct Moodle upload hand-in mechanism. You are advised to check your work after upload, to make sure it has uploaded properly. **Do not alter your work after the deadline**. You should make at least one full backup copy of your work.

Requirements

It is your responsibility to make sure that your work is complete and available for marking by the deadline. Make sure that you have followed the submission instructions carefully, and your work is submitted in the correct format, using the correct hand-in mechanism (e.g., Moodle upload). When submitting via Moodle, you are advised to check your work after upload, to make sure it has uploaded properly. Do not alter your work after the deadline. You should make at least one full backup copy of your work.

You are required to submit your work in the form of a **single PDF file**.

Penalties for late submission

The timeliness of submissions is strictly monitored and enforced.

All coursework has a late submission window of 7 calendar days, but any work submitted within the late window will be capped at 40%, unless you have an agreed extension. Work submitted after the 7-day late window will be capped at zero unless you have an agreed extension. See 'Assessment Mitigation' below for further information on extensions.

Please note that individual tutors are unable to grant any extensions to assessments.

Assessment Mitigation

If there is a valid reason why you are unable to submit your assessment by the deadline you may apply for Assessment Mitigation. There are two types of mitigation you can apply for via the module area on Moodle (in the 'Assessments' block on the right-hand side of the page):

- **Non-evidenced extension**: does **not** require you to submit evidence. It allows you to add a **short** extension to a deadline. This is not available for event-based assessments such as in-class tests, presentations, interviews, etc. You can apply for this extension during the assessment weeks, and the request must be made **before** the submission deadline. For this assessment, the non-evidenced extension is 2 days.

- **Evidenced extension**: requires you to provide independent evidence of a situation which has impacted you. Allows you to apply for a longer extension and is available for event-based assessment such as in-class test, presentations, interviews, etc. For event-based assessments, the normal outcome is that the assessment will be deferred to the summer reassessment period.

Further information about Assessment Mitigation is available on the dedicated Assessments page at `https://www.mmu.ac.uk/student-life/course/assessments`.

Personal Learning Plans (PLP)

If you have a Personal Learning Plan (PLP) which states you can negotiate an extended deadline, then if you need to you can submit an evidenced extension request on the Moodle site for the module.

Plagiarism

Plagiarism is the unacknowledged representation of another person's work, or use of their ideas, as one's own. Manchester Metropolitan University takes care to detect plagiarism, employs plagiarism detection software, and imposes severe penalties, as outlined in the Student Code of Conduct and Academic Misconduct Policy. Poor referencing or submitting the wrong assignment may still be treated as plagiarism. If in doubt, seek advice from your tutor.

As part of a plagiarism check, you may be asked to attend a meeting with the Module Leader, or another member of the module delivery team, where you will be asked to explain your work (e.g. explain the code in a programming assignment). If you are called to one of these meetings, it is very important that you attend.

Use of generative AI

The use of generative AI is permitted in this assessment, so long as it is used in accordance with the instructions provided in the 'Are you allowed to use AI in assessments?' section of the AI Literacy Rise Study Pack. **All submitted work must be your own original content.** We recommend working to the two main principles:

1. You should always authentically represent your capabilities.
2. You should never trust the outputs of Generative AI uncritically.

Specifically, when it comes to this assessment, you:

- Can use generative AI to help you understand the assessment and the associated content, but you must check this against other sources.
- Can use generative AI as part of the planning process (e.g. to get ideas, to break down tasks, to explore different structures).
- Can use generative AI to find information but should not consider it a reliable source.
- Can use generative AI to provide feedback on your work. But you must maintain authorship by deciding about each change suggested.
- **Cannot use it to create the assessment submission itself.**

If you are unable to upload your work to Moodle

If you have problems submitting your work through Moodle, you can raise a ticket with the Assessment Management Team using the Assist Portal. This must be done before the published deadline, else your work will be logged as a late submission.

Assessment Regulations

For further information see the Undergraduate Assessment Regulations on the Assessments and Results information pages

Support and feedback

Your work on this coursework will be supported by the lectures and tutorial sessions for the unit. If you wish to contact Killian outside of class then see the Moodle area for his office hours and contact details.

Summative feedback will be given in the form of markings and comments on your submitted work when returned.

Department of Computing and Mathematics

Number Theory questions

1. Consider your eight-digit MMU student identification number. Let a be the integer formed by the rightmost four digits of your ID number and let b be the integer formed by the leftmost four digits. (*For example, the ID number* 11045630 *produces* $a = 5630$ *and* $b = 1104$)

   (a) Use the Euclidean algorithm to find gcd(a, b) and integer coefficients m, n that satisfy

   $$\text{gcd}(a, b) = ma + nb.$$

   Your answer should show all the steps of the algorithm and briefly explain why the number produced is the required greatest common divisor.

   [8]

   (b) Give the prime factorizations of a and b and explain how these confirm the value of gcd(a, b) produced by the algorithm.

   [3]

   (c) If $x, y, z \in \mathbb{Z}$ let d be the smallest positive integer that can be expressed in the form

   $$0 < d = \alpha x + \beta y + \gamma z,$$

   where $\alpha, \beta, \gamma \in \mathbb{Z}$. Describe how the Euclidean algorithm can be extended to find $\gcd(x, y, z)$ and coefficients α, β and γ giving d as above.

   Give values for one choice of α, β and γ that produce d when $x = a$, $y = b$ (the numbers extracted from your ID) and $z = 10007$.

   [3]

   (d) Assuming they make no mistakes, why is it that everyone in the class will obtain the same value for d in part (c)? What is the smallest choice of integer $z > 1$ where you can be certain that everyone in the class will obtain the same value for d?

   The eight-digit MMU ID numbers begin with the two-digit year when the student first registered with the university. You will assume that everyone in the class has an ID number in the range 21000000 $\leq ID \leq$ 24999999. *You should assume no other knowledge about anyone's ID number.*

   [3]

Number Theory questions

2. Let n be the integer given by your eight-digit MMU student ID number.

   (a) What is the remainder produced when the integer 2026^n is divided by 73?

   [8]

   (b) What is the remainder produced when the integer 2026^{2027^n} is divided by 73? Be careful to interpret the tower of powers correctly, i.e. $2026^{2027^n} = 2026^{\left(2027^n\right)}$.

   [4]

   (c) The number of different possible answers to part (b), that students in the class will find, is quite a small number, less than ten. Find this number and explain why this is the case.

   [3]

   Your solutions should show how concepts and results from the unit about congruences allow one to find these remainders whilst avoiding, as far as possible, explicitly evaluating large integers.

3. Consider the sequence of positive integers a_n, for $n \geq 1$, defined by

$$a_n = 10^{(2^n)} + 1.$$

   (a) Prove that the elements of this sequence are pairwise coprime, i.e. prove that if $m \neq n$ then gcd$(a_m, a_n) = 1$.

   [9]

   (b) Show how this result, combined with the Fundamental Theorem of Arithmetic, provides another proof that there are an infinite number of primes.

   [3]

   Hint: *Begin the first part by proving that* $a_n | (a_{n+1} - 2)$ *and then try to extend this divisibility result in a useful way.*

4. Consider a general arithmetic sequence $x_j = y + jn$, $(j \geq 1)$. Prove that if p is a prime number such that $p \not| n$ then there is some element from the sequence $\{x_j\}_{j=1}^{\infty}$ that is divisible by p.

   Hint: *To prove this result you will need to consider the divisibility of the sequence elements using the concept of the congruence relation and modular arithmetic on the integers.*

   Your proof of this result should give you a method which, for a given arithmetic sequence and prime, actually allows you to calculate a point in the sequence at which the divisibility property holds. Illustrate your method by calculating the first element from this sequence that is divisible by p, where

$$p = 150000001 = 1.5 \times 10^8 + 1,$$

   n is the integer represented by your ID number and $y = 2026$.

   [6]

Group Theory questions

5. *Permutation groups and dihedral groups*

   Let n be a positive integer greater than 2. The dihedral group D_n is the symmetry group of a regular n-sided polygon centred at the origin. It is generated by a rotation, r, counter-clockwise about the origin through an angle $2\pi/n$, and a reflection s, in an axis running through one of the polygon's vertices and the origin. These generators for D_n are subject to the relations $r^n = e$, $s^2 = e$ and $sr = r^{-1}s$. Each element of D_n can be expressed in the standard form $r^i s^j$, where $0 \leq i \leq n-1$ and $j = 0$ or 1.

   (a) For which values of n is the alternating group A_n abelian and for which n is it nonabelian? Justify your answer.

   [5]

   (b) For which values of n is the dihedral group D_n abelian and for which n is it nonabelian? Justify your answer.

   [5]

   (c) The **centre** of a group G is

   $$Z(G) = \{g \in G : gx = xg \text{ for all } x \in G\}.$$

   What is the centre of D_n? Your answer should deal with all posible values for $n \geq 3$.

   [5]

6. *Subgroups of dihedral groups*

   A group G is *Lagrangian* if for every positive divisor d of $|G|$ there is a subgroup H of G with $|H| = d$.

   (a) Give a complete description of the subgroups of D_n for all $n \geq 2$. Your description should detail the elements of each subgroup, prove that they are subgroups and prove that there are no other subgroups apart from the ones you describe.

   [10]

   (b) Explain how your treatment confirms the fact that the dihedral groups are Lagrangian.

   [5]

   (c) Use the `.subgroups()` and `.order()` methods of Sage to determine the number and orders of all the subgroups of a few examples of D_n in order to validate the work you've done in part (a).

   [5]

   (d) Prove which of the subgroups are normal in D_n.

   [5]

Group Theory questions

7. *The importance of normal subgroups and factor groups*

Normal subgroups and the factor group construction provide a way to get a simplified view of a group G by partitioning its elements into subsets and looking at the operation induced on the partition by the operation from G. In this question you will prove that normal subgroups are the only such way to obtain simplified views of G.

A *congruence* on a group G is an equivalence $\sim$ on G that is compatible with the group operation of G, in the sense that, if $g_1 \sim g_2$ and $h_1 \sim h_2$ then $g_1h_1 \sim g_2h_2$.

Let $\sim$ be a congruence on G.

(a) Prove that if $g_1 \sim g_2$ then $g_1^{-1} \sim g_2^{-1}$.

[3]

(b) Prove that the partition of G induced by the equivalence classes of $\sim$ is the partition of G into the cosets of a certain normal subgroup of G. Your answer should include a clear definition of this normal subgroup N, defined with reference to $\sim$, and prove that it is a normal subgroup of G.

[7]