Department of Computing and Mathematics Semester 2
Coursework assignment cover sheet Academic Year 2023/24

Unit code and title	6G5Z3048 Number Theory and Abstract Algebra
Assignment set by	Dr Killian O'Brien
Assignment ID	1CWK40
Assignment weighting	40%
Assessment Title	Coursework
Type	Individual
Hand-in deadline	See Moodle
Hand-in format and mechanism	Single PDF file to the Moodle submission point

Learning outcomes 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.

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). If 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.

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 below for further information on extensions.

Please note that individual tutors are unable to grant extensions to coursework.

Self-certification and evidenced extensions

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

- Self-certification: does not require you to submit evidence. Allows you to add a short extension (usually, but not always, seven days) to a deadline. This is not available for event-based assessments such as in-class test, presentations, interviews, etc. You can apply for this extension during the assessment weeks, and the request must be made before the submission deadline.
- Evidenced extensions: 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 resit period.

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 Handbook (`http://www.mmu.ac.uk/academic/casqe/regulations/docs/policies_regulations.pdf` and Regulations for Undergraduate Programmes (`https://www.mmu.ac.uk/academic/casqe/regulations/assessment/docs/ug-regs.pdf`). Bad referencing or submitting the wrong assignment may still be treated as plagiarism. If in doubt, seek advice from your tutor.

If you are unable to upload your work to Moodle

If you have problems submitting your work through Moodle you can email it to the Assessment Team's Contingency Submission Inbox using the email address `submit@mmu.ac.uk`. You should say in your email which unit the work is for, and ideally provide the name of the Unit Leader. The Assessment team will then forward your work to the appropriate person. If you use this submission method, your work must be emailed by the published deadline, or it will be logged as a late submission.

Assessment Regulations

For further information see Assessment Regulations for Undergraduate/Postgraduate Programmes of Study on the Student Life web pages at this address

`https://www.mmu.ac.uk/student-life/course/assessments#ai-63930-2`.

As part of a plagiarism check, you may be asked to attend a meeting with the Unit Leader, or another member of the unit 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.

Support

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

Feedback

Feedback on your submissions will be provided in the form of detailed comments and marks on your submitted PDF, returned to you with your marks.

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?

You can assume that the eight-digit MMU ID numbers begin with the two-digit year when the student first registered with the university, so most people in the class have a number of the form 22xxxxxx *or* 21xxxxxx. *Everyone in the class has an ID number in the range* 15000000 $\leq ID \leq$ 22999999. *You should assume no other knowledge about anyone's ID number.*

[3]

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

(a) What is the remainder produced when the integer 2024^n is divided by 73?

[8]

(b) What is the remainder produced when the integer 2024^{2023^n} is divided by 73? Be careful to interpret the tower of powers correctly, i.e. $2024^{2023^n} = 2024^{\left(2023^n\right)}$.

[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.

Number Theory questions

(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 from 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 $y = 2024$.

[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.

[6]

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

[6]

(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?

[4]

(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 form the ones you describe.

[12]

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

[4]

(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).

[4]

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

[4]

(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 $g_1 h_1 \sim g_2 h_2$.

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.

[7]