Manchester Metropolitan University

Mock Examination 02
Faculty Of Science & Engineering
Department Of Computing And Mathematics
MATHEMATICS UNDERGRADUATE NETWORK
Level 5

Mock examination 02 for

6G5Z0048 Number Theory and Abstract Algebra

Duration : 3 hours

Instructions to students

- You need to answer **FIVE** questions. This must include **TWO** questions from Section A and **TWO** questions from Section B. Your fifth question can then come from any of the remaining questions.
- If you answer more than five questions then you will get the marks from your best five questions, subject to the sectioning requirements above.
- You must show all of your working and explain your reasoning carefully to gain full marks.
- Marks awarded for each question part are shown in square brackets aligned to the right-hand margin.

Permitted materials

- Students are permitted to use their own calculators without mobile communication facilities.

SECTION A – Number Theory questions

1. (a) State precisely the definition of the divisibility relation $a\,|b$ on the integers and use it to prove that the relation is transitive, i.e. [6]

$$(a|b \ \& \ b|c) \Rightarrow a|c.$$

(b) Write down the definition of $\gcd(a, b)$. How is the value of $\gcd(a, b)$ characterised in tewrms of linear combinations of the two integers a and b? [5]

(c) Use the Euclidean Algorithm to calculate $gcd(136, 36)$. Give brief explanations for the main steps of the algorithm and explain why the output produced is the gcd. [4]

(d) Use the principle of mathematical induction to prove that [5]

$$\forall n \geq 1 \quad 8\,|\left(3^{2n} + 7\right).$$

2. (a) Prove that there are infinitely many prime numbers (Euclid's theorem). State clearly any results about divisibility that you make use of. [10]

(b) What are the possible remainders r left when a prime p is divided by 8 as in [5]

$$p = 8q + r, \quad (0 \leq r < 8)?$$

Hence prove that the integer $p^2 - 1$ is never a prime for any prime $p > 2$.

(c) Prove that if $2^n - 1$ is prime then n is prime. (Hint: Prove the contra-positive). [5]

SECTION A – Number Theory questions

3. (a) Carefully state the definition of the relation $a \equiv b \pmod{n}$. How does it relate to the remainders produced when a and b are divided by n? [3]

   (b) Suppose that $ac \equiv bc \pmod{m}$ and that $d = \gcd(c, m)$. Prove that [10]

$$a \equiv b \pmod{\frac{m}{d}}.$$

   (c) What is the remainder left when 2013^{2013} is divided by 10? In your solution you should exploit the properties of congruence to avoid as far as possible the direct evaluation of large integers. [7]

4. (a) Consider the congruence [7]

$$30x \equiv 18 \pmod{84}.$$

   User relevant result(s) from the theory of congruences to find all the solutions.

   (b) Use the Chinese Remainder Theorem to describe the integers x that satisfy all three of the following congruences simultaneously, [7]

$$\begin{aligned} x &\equiv 2 \pmod{5} \\ x &\equiv 5 \pmod{11} \\ x &\equiv 9 \pmod{13}. \end{aligned}$$

   Your final answer should be in the form of a single congruence class for x modulo an appropriate modulus.

   (c) Use the Legendre symbol, the law of quadratic reciprocity and other relevant properties to show that there are no integer solutions to the congruence [6]

$$x^2 \equiv 503 \pmod{631}.$$

   (You can use the fact that 503 and 631 are both prime.)

End of Section A

SECTION B – Abstract Algebra questions

5. (a) Let G be a non-empty set and $*$ a binary operation on G, i.e. [6]

$$\forall\, g_1, g_2 \in G \quad g_1 * g_2 \in G.$$

State the three extra conditions that the pair $(G, *)$ needs to satisfy in order to be called a *group* and explain their meaning. Illustrate each condition with an example drawn from the pair $(\mathbb{Z}, +)$.

(b) Explain why the pair $(\mathbb{R}, \times)$, consisting of the real numbers and the operation of multiplication does not form a group. What modification is needed to $\mathbb{R}$ so that a group can be formed with the operation $\times$? [2]

(c) Which matrices are elements of the group GL$(n, \mathbb{R})$? Prove that this is a group under the operation of matrix multiplication. Clearly state any properties of matrices that you use. [7]

(d) Consider the set of 3×3 upper-triangular matrices $H \subset$ GL$(n, \mathbb{R})$ given by [5]

$$H = \left\{ \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \;:\; x, y, z \in \mathbb{R} \right\}.$$

Prove that H forms a subgroup of GL$(n, \mathbb{R})$.

6. (a) Suppose that G is a group. State the definition of the terms *subgroup* of G and *order*, $|g|$, of an element of G. [5]

(b) Let $C_n = \langle a \rangle$ denote the cyclic group of order n generated by an element a and written using multiplicative notation, so that

$$C_n = \{e, a, a^2, a^3, \ldots, a^{n-1}\}.$$

(i) Prove that every subgroup H of C_n is cyclic by proving that $H = \langle a^k \rangle$, where k is the smallest non-negative integer such that $a^k \in H$. [6]

(ii) Prove that $a^m = e$ if and only if $n|m$, i.e. n divides m. [3]

(iii) If $b = a^r$ then prove that the order of b in C_n is n/d where $d = \gcd(r, n)$. [3]

(iv) Illustrate these results by determining the elements of *all* the subgroups of the cyclic group, $C_{20} = \langle a \rangle$, the cyclic group of order 20. [3]

7. (a) State Lagrange's theorem on the orders of subgroups of a finite group G. [2]

   (b) Let H be a subgroup of a finite group G.

      (i) State the definition of the *left* and *right cosets* of H in G. [2]

      (ii) Let $g_1, g_2 \in G$. Prove that the left-cosets g_1H and g_2H are either equal or disjoint, i.e. [3]

$$g_1H = g_2H \quad \text{or} \quad g_1H \cap g_2H = \emptyset.$$

      (iii) Prove that all cosets of H in G contain the same number of elements. [3]

      (iv) Then show how parts (ii) and (iii) above can be used to prove Lagrange's theorem. [3]

   (c) Suppose that G is a group of prime order. Use Lagrange's theorem to prove that G is cyclic. [7]

8. (a) Define what is meant by a *normal subgroup* of a group G. [2]

   (b) The dihedral group D_n, the group of symmetries of a regular polygon with n sides, is generated by two elements r, a rotation, and s, a reflection. These are subject to the relations $r^n = e, s^2 = e$ and $sr = r^{-1}s$. The $2n$ elements of D_n can be expressed in the standard form $r^i s^j$, where $0 \leq i \leq n-1$ and $j = 0, 1$.

      (i) Prove that $H = \{e, r^3\}$ is a normal subgroup of D_6. [3]

      (ii) What will be the order of the factor group D_6/H? [1]

      (iii) Determine the elements of each of the left-cosets of H in D_6. [4]

      (iv) Assign suitable labels to the cosets and construct a Cayley table for the factor group D_6/H. [4]

      (v) Use your Cayley table to explain why the factor group D_6/H is isomorphic to another dihedral group D_n. [4]

   (c) Suppose that H and K are normal subgroups of a group G and that $H \cap K = \{e\}$. By carefully considering the commutator $hkh^{-1}k^{-1}$ prove that elements of H and K commute with one another, i.e. [4]

$$\forall\, h \in H \;\forall\, k \in K \quad hk = kh.$$

End of Section B

End OF QUESTIONS