

DEGREE EXAMINATION

MA2002 Discrete Mathematics and Algebraic Structures

Monday 22 January 2001

(9am to 11am)

Only calculators approved by the Department of Mathematical Sciences may be used in this examination. Calculator memories must be clear at the start of the examination.

Marks may be deducted for answers that do not show clearly how the solution is reached.

Answer ALL FOUR questions.

The set of integers modulo n is denoted by \mathbb{Z}/n . The set \mathbb{N} of natural numbers includes 0.

1. (a) Use the Extended Euclidean Algorithm to calculate the highest common factor, $\text{hcf}(a, b)$, of $a = 132$ and $b = 372$ and express it in the form $as + bt$, where $s, t \in \mathbb{Z}$.

Find all the solutions (x, y) in integers of the Diophantine equation

$$132x + 372y = 24.$$

- (b) The solutions (x, y) in integers of the equation

$$51x + 43y = 2130$$

are given by $(x, y) = (-34080 + 43k, 40470 - 51k)$, ($k \in \mathbb{Z}$). Using this result, which you are not expected to prove, find all those solutions with $x \geq 0$ and $y \geq 0$.

- (c) Let a and b be two positive integers such that a does not divide b . Using the Division Algorithm we can write $b = qa + r$, where $q, r \in \mathbb{Z}$ and $0 < r < a$. (You are not expected to justify this assertion.)

Prove that

$$\text{hcf}(b, a) = \text{hcf}(a, r).$$

2. (a) Find the inverse of the unit $[4]_{11}$ in $\mathbb{Z}/11$. Hence, or otherwise, solve the following equation for $[x]_{11}$ in $\mathbb{Z}/11$

$$[4]_{11} \cdot [x]_{11} = [6]_{11}.$$

- (b) Solve the simultaneous congruence equations

$$x \equiv 6 \pmod{13}, \quad 2x \equiv 3 \pmod{5}.$$

- (c) What is meant by saying that a positive integer is *prime*? State the Fundamental Theorem of Arithmetic (that is, the Unique Factorization Theorem for \mathbb{Z}).

Express each of the integers 1200 and 630 as a product of prime powers. Hence write down their highest common factor, $\text{hcf}(1200, 630)$, and least common multiple, $\text{lcm}(1200, 630)$.

Let $n > 1$ be an integer which is not divisible by any prime number p such that $p^2 \leq n$. Use the Fundamental Theorem to show that n is prime.

3. (a) State, without giving a proof, which of the following three mappings $f_i : \mathbb{N} \rightarrow \mathbb{N}$, ($i = 1, 2, 3$), are injective, which are surjective, and which are bijective.

(i) $f_1(n) = n + 5$;

(ii) $f_2(n) = n + (-1)^n$;

(iii) $f_3(n) = \begin{cases} n/2 & \text{if } n \text{ is even,} \\ (n-1)/2 & \text{if } n \text{ is odd.} \end{cases}$

Let $A = \{1, 2, 3\}$, $B = \{-2, -1, 0, 1, 2\}$, $C = \{4, 5, 6\}$, and let $f : A \rightarrow B$ and $g : B \rightarrow C$ be the mappings given by

$$\begin{aligned} f(1) = 0, \quad f(2) = -1, \quad f(3) = 2; \\ g(-2) = 6, \quad g(-1) = 4, \quad g(0) = 5, \quad g(1) = 4, \quad g(2) = 6. \end{aligned}$$

Calculate the composition $h = g \circ f : A \rightarrow C$. Given that h is a bijection, find its inverse $h^{-1} : C \rightarrow A$.

- (b) Let $V = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ and let

$$E = \{\{1, 3\}, \{2, 7\}, \{3, 9\}, \{4, 6\}, \{5, 7\}, \{5, 8\}, \{7, 8\}\}.$$

An equivalence relation \sim is defined on the set V by

$x \sim y$ if and only if there exist elements v_0, v_1, \dots, v_n in V , for some $n \geq 0$, such that $x = v_0$, $y = v_n$, and $\{v_{i-1}, v_i\} \in E$ for $1 \leq i \leq n$.

Say briefly why \sim is an equivalence relation and determine the equivalence classes.

- (c) Let $f : X \rightarrow Y$ and $g : Y \rightarrow Z$ be mappings (between sets X, Y and Z). Prove the following results about the composition $g \circ f : X \rightarrow Z$.

(i) If f and g are injective, then $g \circ f$ is injective.

(ii) If $g \circ f$ is injective, then f is injective.

4. (a) State Fermat's (Little) Theorem.

Hence, or otherwise, find the order of $[8]_{19}$ in the group of units in $\mathbb{Z}/19$.

What is the remainder when 3^{180002} is divided by 19?

- (b) Let σ be the permutation of $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ given by

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 9 & 5 & 7 & 1 & 8 & 6 & 4 & 2 \end{pmatrix}.$$

Express σ as a product of disjoint cycles. Hence find the order of σ in the permutation group.

- (c) With the help of a diagram, describe the symmetries of an equilateral triangle. Express the elements of the symmetry group in terms of two generators, and give the order of each element. Give three relations, satisfied by the generators, which determine the group multiplication.