UNIVERSITY OF ABERDEEN **SESSION 2003–04**

DEGREE EXAMINATION

MA2002 Discrete Mathematics and Algebraic Structures

Monday 16 August 2004 (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. All questions carry equal weight.

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, $\mathrm{hcf}(a, b)$, of $a = 264$ and $b = 209$ and express it in the form $as + bt$, where s, $t \in \mathbb{Z}$.

From your calculation, write down the continued fraction expansion of the rational number $a/b = 264/209$.

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

$$264x + 209y = 22\,.$$

(b) 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, $\mathrm{hcf}(1200, 630)$, and least common multiple, $\mathrm{lcm}(1200, 630)$.

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

Prove that

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

2. **(a)** Find the inverse of the unit $[13]_{19}$ in $\mathbb{Z}/19$. Hence, or otherwise, solve the following equation for $[x]_{19}$ in $\mathbb{Z}/19$:

$$[13]_{19} \cdot [x]_{19} = [4]_{19}.$$

(b) Solve the simultaneous congruence equations:

$$x \equiv 5 \,(\mathrm{mod}\, 11), \qquad 2x \equiv 1 \,(\mathrm{mod}\, 7).$$

(c) What is meant by saying that a positive integer $p \geq 1$ is *prime*?

Suppose that p is a prime number. Say, briefly, why, if $p > 3$, then either $p \equiv 1 \pmod 6$ or $p \equiv 5 \pmod 6$.

Let $m \geq 1$ be a positive integer, and write $M = m!$. By considering the factorization of $n = 6M - 1$ as a product of primes, prove that there is a prime number p such that $m < p \leq 6M - 1$ and $p \equiv 5 \pmod 6$.

3. **(a)** For each of the following mappings, say whether it is injective (yes or no) and whether it is surjective (yes or no). Give a brief reason for each answer.

(i) $\mathbb{Z} \to \mathbb{Z} : x \mapsto 3x - 1$;

(ii) $\mathbb{Z}/6 \to \mathbb{Z}/6 : [n]_6 \mapsto [5n]_6$;

(iii) $\mathbb{N} \times \mathbb{N} \to \mathbb{N} : (m, n) \mapsto 4^m \cdot 8^n$;

(iv) $\mathbb{Z} \to \mathbb{N} : n \mapsto \begin{cases} 2n & \text{if } n \geq 0, \\ -(2n+1) & \text{if } n < 0. \end{cases}$

(b) Let $A = \{0, 1, 2, 3, 4\}$, $B = \{0, 2, 4\}$, $C = \{1, 3, 5, 7\}$, and let $f : A \to B$ and $g : B \to C$ be the mappings given by

$$f(0) = 4, \quad f(1) = 0, \quad f(2) = 0, \quad f(3) = 4, \quad f(4) = 2;$$
$$g(0) = 7, \quad g(2) = 1, \quad g(4) = 5.$$

Calculate the composition $g \circ f : A \to C$.

Say which of the three mappings f, g and $g \circ f$ are injective and which are surjective.

Find a mapping $h : B \to A$ such that $f(h(y)) = y$ for all elements $y \in B$ of the set B.

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

(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 S_9. What is the order of σ^{-1}?

(c) Let $n > 1$ be a positive integer. What is meant by saying that $[a]_n$ is a *zero-divisor* in $\mathbb{Z}/n$?

Giving reasons, determine which of the following elements of $\mathbb{Z}/24$ are zero-divisors:

$$[6]_{24}, \quad [5]_{24}, \quad [4]_{24}.$$

An element $[a]_n \in \mathbb{Z}/n$ is said to be *nilpotent* if there is an integer $k \geq 1$ such that $[a]_n^k = [0]_n$. Prove that a non-zero nilpotent element in $\mathbb{Z}/n$ is a zero-divisor.

Determine whether any of the elements of $\mathbb{Z}/24$ listed above is nilpotent. Justify your answer.