UNIVERSITY OF ABERDEEN **SESSION 2004–05**

Degree Examination

MA2002 Discrete Mathematics and Algebraic Structures

Wednesday 19 January 2005 (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, $\text{hcf}(a, b)$, of $a = 1002$ and $b = 903$ 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 $a/b = 1002/903$.

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

$$1002x + 903y = 30\,.$$

(b) What is meant by saying that a positive integer $p \geq 1$ is prime? State the Fundamental Theorem of Arithmetic (that is, the Unique Factorization Theorem for $\mathbb{Z}$).

Express each of the integers $24,000$ and $24,750$ as a product of prime powers. Hence write down their highest common factor, $\text{hcf}(24000, 24750)$, and least common multiple, $\text{lcm}(24000, 24750)$.

Let $n > 1$ be an integer that is not divisible by any prime number p such that $p^2 \leq n$. Using the Fundamental Theorem, or otherwise, prove that n is prime.

(c) Recall that, for a prime $p > 1$ and positive integer $n \geq 1$, the *p-adic valuation* $\nu_p(n)$ is defined to be the greatest integer $r \geq 0$ such that p^r divides n.

Determine $\nu_{257}(1000!)$.

2. **(a)** Find the inverse of the unit $[10]_{29}$ in $\mathbb{Z}/29$. Hence, or otherwise, solve the following equation for $[x]_{29}$ in $\mathbb{Z}/29$:

$$[10]_{29} \cdot [x]_{29} = [15]_{29}.$$

(b) Solve the simultaneous congruence equations:

$$x \equiv 7 \,(\mathrm{mod}\, 19), \qquad x \equiv 3 \,(\mathrm{mod}\, 11).$$

(c) A non-negative integer x is written to the base 8 as

$$x = a_r 8^r + \ldots + a_1 8^1 + a_0 8^0 \quad (= \sum_{j=0}^{r} a_j 8^j),$$

where $a_j \in \mathbb{Z}$ and $0 \le a_j < 8$ for $j = 0, \ldots, r$. Let $y = a_r + \ldots + a_1 + a_0$ $(= \sum_{j=0}^{r} a_j)$ be the sum of the digits.

By doing arithmetic (mod 7), or otherwise, prove that x is divisible by 7 if and only if y is divisible by 7.

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) $\mathbb{N} \to \mathbb{N} : x \mapsto x + 5$;

(ii) $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} : (m, n) \mapsto 3m - 2n$;

(iii) $\mathbb{Z}/10 \to \mathbb{Z}/10 : [x]_{10} \mapsto [2x]_{10}$;

(iv) $\{0,\, 1\} \times \mathbb{N} \to \mathbb{N} : (m, n) \mapsto 2n + m$.

(b) Let $A = \{0, 2, 4, 6\}$, $B = \{1, 3, 5, 7, 9\}$, $C = \{1, 2, 3, 4\}$, and let $f : A \to B$ and $g : B \to C$ be the mappings given by

$$f(0) = 1,\ f(2) = 5,\ f(4) = 3,\ f(6) = 9;$$
$$g(1) = 4,\ g(3) = 2,\ g(5) = 3,\ g(7) = 2,\ g(9) = 1.$$

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

(c) Define the term *equivalence relation* on a set X.

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

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

Draw the graph with vertices the elements $v \in V$ and edges the elements $\{u, v\} \in E$.

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

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

Give brief reasons to justify the assertion that $\sim$ is an equivalence relation.

Find the equivalence classes of $\sim$.

4. **(a)** Find the order of the unit $[8]_{15}$ in $\mathbb{Z}/15$.

What is the remainder when 8^{12345} is divided by 15?

(b) State Fermat's (Little) Theorem.

Hence, or otherwise, find the order of the unit $[2]_{89}$ in $\mathbb{Z}/89$.

Let p and q be distinct primes (> 1). Write $n = pq$ and $k = \mathrm{lcm}(p-1, q-1)$ (the least common multiple of $p-1$ and $q-1$).

Using Fermat's theorem, prove that

$$[a]_n^k = [1]_n$$

for each unit $[a]_n$ in $\mathbb{Z}/n$.

(c) Let $n > 1$ be an integer and let $\pi \in S_n$ be a permutation of $\{1, 2, \ldots, n\}$. Define the *order* of π.

Let $\sigma \in S_9$ be the permutation of $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ given by

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

Express σ as a product of disjoint cycles, illustrating the cycle decomposition by a diagram. Hence find the order of σ in the permutation group.

Write the permutation σ^3 as a product of disjoint cycles and hence determine its order.