UNIVERSITY OF ABERDEEN **SESSION 2003-04**

DEGREE EXAMINATION

MA2002 Discrete Mathematics and Algebraic Structures

Monday 26 January 2004 (3pm to 5pm)

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 $a = 294$ and $b = 77$ 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 $a/b = 294/77$.

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

$$294x + 77y = 35\,.$$

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

$$295x + 187y = 6000$$

are given by $(x, y) = (426000 + 187k, -672000 - 295k)$, $(k \in \mathbb{Z})$. Using this result, which you are not expected to prove, find all those solutions with $x \geq 0$ and $y \geq 0$.

(c) State the Fundamental Theorem of Arithmetic (that is, the Unique Factorization Theorem for $\mathbb{Z}$).

Using the theorem

(i) determine the number of positive integers (≥ 1) that divide the integer

$$n = 151200\,;$$

(ii) prove that, for any positive integer $m \geq 1$, there is a prime number p such that

$$m < p \leq m! + 1.$$

2. **(a)** Find the inverse of the unit $[10]_{13}$ in $\mathbb{Z}/13$. Hence, or otherwise, solve the following equation for $[x]_{13}$ in $\mathbb{Z}/13$:

$$[10]_{13} \cdot [x]_{13} = [11]_{13}.$$

(b) Using, without proof, the fact that

$$-42(104) + 17(257) = 1,$$

deduce that $[104]_{257}$ is a unit in $\mathbb{Z}/257$ and write down its inverse.

(c) Solve the simultaneous congruence equations:

$$x \equiv 2 \,(\mathrm{mod}\, 11), \qquad x \equiv 5 \,(\mathrm{mod}\, 13).$$

(d) Let Y be the set $\mathbb{Z}/4$ of integers (mod 4), and let $X = Y \times Y$. How many elements has the set X?

A relation $\sim$ is defined on X by

$$([a]_4, [b]_4) \sim ([c]_4, [d]_4) \quad \text{if and only if} \quad [a]_4 + [b]_4 = [c]_4 + [d]_4 \,.$$

Show that $\sim$ is an equivalence relation and list the equivalence classes.

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) $\mathbb{Q} \to \mathbb{Q} : \; x \mapsto 3x - 1 \,;$

(ii) $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} : \; (m, n) \mapsto 3m + 5n;$

(iii) $\mathbb{N} \times \mathbb{N} \to \mathbb{N} : \; (m, n) \mapsto 3^m \cdot 5^n \,;$

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

(b) Let $A = \{1, 2, 3, 4\}$, $B = \{0, 2, 4, 6, 8\}$, $C = \{6, 7, 8, 9\}$, and let $f : A \to B$ and $g : B \to C$ be the mappings given by

$$f(1) = 4,\ f(2) = 0,\ f(3) = 8,\ f(4) = 2;$$
$$g(0) = 6,\ g(2) = 7,\ g(4) = 9,\ g(6) = 9,\ g(8) = 8.$$

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) 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 surjective, then $g \circ f$ is surjective.

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

4. **(a)** Let $n > 1$ be an integer and let $[a]_n$ be a unit in $\mathbb{Z}/n$. Define the term (multiplicative) *order* of the unit $[a]_n$.

Find the order of the unit $[7]_{10}$ in $\mathbb{Z}/10$.

What is the remainder when 7^{8003} is divided by 10?

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

Hence, or otherwise, find the order of the unit $[60]_{257}$ in $\mathbb{Z}/257$. (You should use the fact that $257 = 2^8 + 1$ is prime.)

(c) Let $\sigma \in S_{11}$ be the permutation of $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ given by

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 3 & 11 & 5 & 8 & 7 & 10 & 9 & 6 & 1 & 4 & 2 \end{pmatrix}.$$

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^2 as a product of disjoint cycles and hence, or otherwise, determine its order.

(d) Let $\pi \in S_n$, where $n > 1$, be a permutation of odd order $2k + 1$. By considering the representation of π as a product of disjoint cycles, or otherwise, show that π^2 has the same order $2k + 1$.