UNIVERSITY OF ABERDEEN **SESSION 2005–06**

DEGREE EXAMINATION

MA2002 Discrete Mathematics

Monday 16 January 2006 (9 am to 11 am)

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 FOUR questions.

1. **(a)** Let a and b be positive integers. Define the **greatest common divisor** of a and b, denoted by $\gcd(a, b)$.

(b) Prove that for a and b as in part (a), $\gcd(a, b)$ may be expressed in the form $sa + tb$ for suitable integers s and t.

(c) Using the Euclidean algorithm, or otherwise, determine $\gcd(1341, 105)$ (you should show your working at each stage).

2. **(a)** State what is meant by saying that the positive integer p is a **prime number**.

(b) Prove that if p is a prime number, and $p \mid ab$ for integers a and b, then either $p \mid a$ or $p \mid b$, stating any general facts about greatest common divisors and divisibility which you make use of.

(c) Let U_{13} denote the group of non-zero elements of $\mathbb{Z}/13\mathbb{Z}$ under multiplication (mod 13). For each of the following elements of U_{13}, find a multiplicative inverse and calculate the order.

i) [7] and ii) [8].

3. **(a)** State Fermat's Little Theorem.

(b) Find the remainder of 2^{176} on division by 13.

(c) State the Chinese Remainder Theorem.

(d) Find an integer A such that $A \equiv 3 \pmod{17}$ and $A \equiv 8 \pmod{125}$.

4. **(a)** Let G be a non-empty set endowed with a binary operation $\circ$. State the properties which must be satisfied for $(G, \circ)$ to be a **group**.

(b) Let n be an integer greater than 1, and let G be the group of all permutations of $\{1, 2, \ldots, n\}$, known as the symmetric group of degree n.

i) State the order of G, and in the case that $n = 3$, give the group table of G.

ii) Suppose now that $n = 5$, and let f be the permutation with

$$f(1) = 3; \quad f(2) = 5; \quad f(3) = 4; \quad f(4) = 1; \quad f(5) = 2.$$

Write down the cycle notation for f, which expresses f as a product of disjoint cycles.

5. Let S be a non-empty set and $\cong$ be a binary relation on S.

(a) State the properties required for $\cong$ to be an equivalence relation on S.

(b) Now consider the case that $S = \mathbb{Z}$ and define $\cong$ via $a \cong b$ if and only if $a - b$ is divisible by 7.

i) Prove that $\cong$ is an equivalence relation on $\mathbb{Z}$.

ii) Explain how to define operations of addition and multiplication on $\mathbb{Z}/7\mathbb{Z}$, which is the set of equivalence classes in i) above, and give the operation tables for both of these operations.