

Degree Examination

MA2002 Discrete Mathematics and Algebraic Structures

Saturday 16 January 1999

(3pm to 5pm)

-----

Answer **ALL FOUR** questions.

Calculators may be used **ONLY** for the arithmetic of real numbers or the numerical evaluation of trigonometric, logarithmic and exponential functions. Calculator memories must be clear at the start of the examination; in particular, the use of pre-stored programs is prohibited. Marks may be deducted for answers that do not show clearly how the solution is reached.

1. (a) Find the highest common factor of 753 and 105 and express it in the form  $753s + 105t$  where  $s$  and  $t$  are integers.

Find all solutions in integers of the Diophantine equation

$$753x + 105y = 15.$$

Find the particular solution for which  $|x|$  is smallest.

Find all congruence classes mod 105 whose members are solutions of

$$753x \equiv 15 \pmod{105}.$$

- (b) Suppose that  $x$ ,  $y$  and  $z$  are positive integers such that  $x$  divides  $z$ ,  $y$  divides  $z$ , and  $x$  and  $y$  are co-prime (that is,  $(x,y) = 1$ ). Prove that  $xy$  divides  $z$ .

2. (a) State the Fundamental Theorem of Arithmetic (concerning the factorization of integers).

Let  $n (\geq 2)$  be an integer that is not prime. Explain why  $n$  has a factor  $a$  such that  $1 < a \leq \sqrt{n}$  and hence show that  $n$  has a prime factor  $p$  such that  $p \leq \sqrt{n}$ . Hence test whether or not 227 is prime.

- (b) In the following list of congruence classes  $[a]_n$ , determine which are units and which are zero divisors.

$$[10]_{12}, [4]_9, [9]_{21}.$$

If  $[a]_n$  is a unit, find both its inverse and its order (with respect to multiplication).

If  $[a]_n$  is a zero divisor, find  $[b]_n \neq [0]_n$  such that  $[a]_n[b]_n = [0]_n$ .

Solve the congruence equation

$$4x \equiv 5 \pmod{9}.$$

**3.** (a) State Fermat's Little Theorem (for a prime  $p$  and an integer  $a$  such that  $(a,p) = 1$ ). Hence, or otherwise, find the (multiplicative) order of  $[2]_{17}$  in  $\mathbb{Z}_{17}$ .

(b) Let  $f: X \rightarrow Y$  be a function. What is meant by saying that  $f$  is injective, and what is meant by saying that  $f$  is surjective?

For each of the following functions, determine whether it is bijective and if it is bijective find a formula for the inverse function.

(i)  $g: \mathbb{Z}_4 \rightarrow \mathbb{Z}_4, \quad g([x]_4) = [2]_4[x]_4.$

(ii)  $h: \mathbb{Z}_5 \rightarrow \mathbb{Z}_5, \quad h([x]_5) = [2]_5[x]_5.$

[Hint. In (ii) you may find it helpful to consider the inverse of  $[2]_5$  in  $\mathbb{Z}_5$ .]

(c) A relation  $R$  is defined on the set  $\mathbb{C}$  of complex numbers by:

$$w R z \text{ if and only if } |w| = |z|.$$

Determine which of the properties of reflexivity, symmetry and transitivity is satisfied by  $R$ .

If  $R$  is an equivalence relation, describe geometrically the equivalence class of  $3 + 4i$ .

**4.** (a) Define what is meant by a group  $G$  with multiplication  $*$ . Suppose that  $(G,*)$  is a group and that  $g,h \in G$ . Write down the inverse of  $g*h$  in terms of  $g^{-1}$  and  $h^{-1}$ , and demonstrate that your answer has the properties required of the inverse.

(b) Let  $\mathbb{R}$  be the set of all real numbers. An operation  $*$  is defined on  $\mathbb{R}$  as follows:

$$x * y = x + y - \sqrt{2}.$$

Find  $e \in \mathbb{R}$  such that  $x * e = x$  for all  $x \in \mathbb{R}$ .

Show that  $(\mathbb{R},*)$  is a group in which the inverse of an element  $x$  is  $2\sqrt{2} - x$ , and show that  $(\mathbb{R},*)$  is Abelian.

(c) In  $S(8)$ , the permutation group on  $\{1,2,3,4,5,6,7,8\}$ , let

$$\pi = (1,5,6,8)(2,5,6,4) \text{ and } \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 7 & 4 & 2 & 6 & 8 & 3 & 1 \end{pmatrix}.$$

Express  $\sigma$  and  $\sigma\pi$  as products of disjoint cycles. Find the order of  $\sigma\pi$ .