G02005

OLLSCOIL NA hÉIREANN, GAILLIMH
THE NATIONAL UNIVERSITY OF IRELAND, GALWAY

SUMMER EXAMINATIONS 2004

FIRST UNIVERSITY EXAMINATION

MATHEMATICS [MA180]

MA183 — *ALGEBRA*

HONOURS
Second Paper

Dr. Dave Johnson
Professor T. Hurley
Dr. J. Burns

Time allowed: *Three* hours.
Answer six questions.

1. Let A be the matrix $\begin{pmatrix} 4 & -6 \\ -2 & 8 \end{pmatrix}$.

(a) Find the eigenvalues and eigenvectors of A.
Write down an invertible matrix E, and a diagonal matrix D, such that $A = EDE^{-1}$.

Calculate A^n and hence or otherwise solve the recurrence relation

$$\begin{array}{rcrcr} x_{n+1} & = & 4x_n & - & 6y_n \\ y_{n+1} & = & -2x_n & + & 8y_n \end{array}$$

given that $x_0 = 2,\ y_0 = 1$.

(b) Write down the transformation $T : \mathbb{R}^2 \to \mathbb{R}^2$ defined by A.
Find the line whose image under T is $x + 2y = 4$, and a line that is fixed by T.

p.t.o.

2. (a) Let

$$A = \begin{pmatrix} -2 & 2 & -3 \\ 2 & 1 & -6 \\ -1 & -2 & 0 \end{pmatrix}.$$

Calculate the inverse A^{-1} of A and use it to solve:

$$-2x + 2y - 3z = 3$$
$$2x + y - 6z = 1$$
$$-x - 2y = 5.$$

(b) Given that $|A^2 - 5A| = 0$, find an eigenvector of A.

(c) Use the cross product to find all the solutions of the system of linear equations

$$-2x_1 + 2x_2 - 3x_3 = 0, \quad 2x_1 + x_2 - 6x_3 = 0.$$

3. (a) State the Well-ordering Axiom for $\mathbb{Z}$, and show that it fails for $\mathbb{Q}$.

(b) Prove by Induction that

$$\frac{1}{2} + \frac{1}{6} + \ldots + \frac{1}{n(n+1)} = \frac{n}{n+1}$$

for all integers $n \geq 1$.

(c) Use Euclid's Algorithm to find the $gcd(1820, 231)$.
Hence, find integers x, y such that $3640x + 462y = 28$.

4. (a) Use the Sieve Method to find all primes in the interval [1,120].

(b) Prove that there are infinitely many primes of the form $4q + 3$, where q is a positive integer.

(c) Prove that $\sqrt{11}$ is irrational.

p.t.o.

5. (a) Find all solutions of the following simultaneous congruences:

$$x \equiv 2 \mod 3$$
$$x \equiv 4 \mod 5$$
$$x \equiv 6 \mod 11$$

(b) Solve the congruence

$$8x \equiv 7 \mod 15$$

and show that the solution is unique module 15.

(c) Find the inverse of 13 in $\mathbb{Z}_{47}$.

6. (a) Define the Euler ϕ function. Show that $\phi(p^n) = p^n(1 - \frac{1}{p})$, where p is a prime. Calculate $\phi(m)$ when (i) $m = 256$ (ii) $m = 2^4.3^7.7^2$.

(b) State (do not prove) Euler's Theorem. Use Euler's Theorem or otherwise to find the remainder when 2^{1014} is divided by 45.

(c) Find the missing digit in the ISBN number

$$4 - 213 - 76? - 35 - 7.$$

7. (a) Write the permutation

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 2 & 7 & 8 & 5 & 10 & 9 & 1 & 3 & 12 & 11 & 4 & 14 & 15 & 13 & 6 \end{pmatrix}$$

(i) as a product of disjoint cycles;
(ii) as a product of transpositions.
Find the *sign* and *order* of π.

(b) Explain how to define a permutation in S_n as either *even* or *odd*. State but do not prove a theorem justifying the *uniqueness* of the definitions of even and odd.

(c) Find the irreducible factors of $x^4 - 1$ in

(i) $\mathbb{Z}_5[x]$, (ii) $\mathbb{Z}_{11}[x]$.

8. Answer <u>one</u> and <u>only one</u> of either **Part A** or **Part B** below.

Part A

(a) State and prove Lagrange's Theorem on the order of a subgroup of a finite group.

(b) Let G be the group of symmetries of a square. List the elements of G. Show that G has two non-isomorphic subgroups of order 4. Write out the multiplication table for each of these subgroups, and explain clearly why they are not isomorphic.

Part B

(a) Let R be a relation on a set S. Explain what is meant by saying that R is an *equivalence relation* on S.

Let $(S, *)$ be an algebraic system. Explain what is meant by saying that R is a *congruence* on $(S, *)$.

Suppose R is a congruence on $(S, *)$ and let $S/R = \{E_a : a \in S\}$ be the set of equivalence classes of S. Define an operation $\overline{*}$ on S/R by $E_a \overline{*} E_b = E_{a*b}$ and show that this operation is unambigously defined (i.e. that it is independent of the class representatives used) and thus that $(S/R, \overline{*})$ is an algebraic system.

(b) Let $S = \mathbb{Z}$ and define aRb if and only if 7 divides $(a-b)$. Show that R is a congruence on both $(\mathbb{Z}, +)$ and $(\mathbb{Z}, \times)$. Describe the algebraic systems $(\mathbb{Z}/R, \overline{+})$ and $(\mathbb{Z}/R, \overline{\times})$.