GX 2106

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

SUMMER EXAMINATIONS 2003

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 $\begin{pmatrix} 2 & -1 \\ -3 & 4 \end{pmatrix}$.

(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

$$\begin{array}{rcrcr} x_{n+1} & = & 2x_n & - & y_n \\ y_{n+1} & = & -3x_n & + & 4y_n \end{array}$$

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 $x + y = 2$.

p.t.o.

2. (a) Let

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

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

$$3x + 6y - 3z = 3$$
$$3x - z = 1$$
$$3x - y = 4.$$

(b) Prove that $\lambda = 2$ is an eigenvalue of A, and find a corresponding eigenvector.

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

$$x_1 + 3x_2 + 4x_3 = 0, \quad 2x_1 + 4x_2 - 3x_3 = 0.$$

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

(b) Use the Principle of Induction to prove that

$$1^2 + 2^2 + 3^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6} \quad \text{for all } n \geq 1.$$

(c) Use Euclid's Algorithm to find the $gcd(250, 111)$.
Hence, find integers x, y such that $250x + 111y = 6$.

4. (a) Use the Sieve Method to find all primes in the interval [8,96].

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

(c) Prove that $\sqrt{7}$ is irrational.

p.t.o.

5. (a) Solve the congruence

$$8x \equiv 7 \pmod{15}$$

and show that the solution is unique modulo 15.

(b) Find the invertible elements of $\mathbb{Z}_9$ stating the inverse of each such element. Solve $5x = 12$ in $\mathbb{Z}_{13}$.

(c) Find the set of *all* solutions to the simultaneous congruences:

$$\begin{aligned} x &\equiv 3 \mod 5 \\ x &\equiv 6 \mod 7 \\ x &\equiv 5 \mod 9 \end{aligned}$$

6. (a) Define the Euler ϕ function.
Calculate $\phi(m)$ when (i) $m = 128$, (ii) $m = 2^4 . 5^{11} . 13^7$.

(b) State and prove *Euler's Theorem.*

Use Euler's Theorem (or otherwise) to find the remainder when 2^{986} is divided by 45.

(c) Find the missing digit in the ISBN number 3-540-7?1-87-X.

7. (a) Write the permutation

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

(i) as a product of disjoint cycles;
(ii) as a product of transpositions.

Find the *order* and the *sign* of π.

(b) Explain how to *uniquely* 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) Factorize x^3+3x^2+x+3 as a product of irreducible polynomials over $\mathbb{Z}_5$.

p.t.o.

8. Answer one and only one 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 $(\mathbb{Z}/R, \overline{\times})$.