UNIVERSITY OF DUBLIN

1417

TRINITY COLLEGE

Faculty of Science

school of mathematics

JS Mathematics **Trinity Term 1996**
SS Mathematics

Course 373

Saturday, June 8 G.M.B. 09.30 — 12.30

Dr. M. Purser and Dr. T.G. Murphy

Answer Section A and B in separate answer books.
Section A - Answer 3 out of the 6 questions
Section B - Answer 2 out of the 4 questions

SECTION B

7. Prove that the multiplicative group $F^\times = F - \{0\}$ of a finite field F is cyclic.

   Find all the generators of $\mathbf{GF}(17)^\times$. How many generators does $\mathbf{GF}(64)^\times$ possess?

8. Listing the elements of $\mathbf{GF}(9)$ in any way you wish, draw up the addition and multiplication tables for this field.

9. Define the *characteristic* of a field, and show that the characteristic of a finite field F is always a prime number.

   Show that a finite field F of characteristic p contains p^n elements for some n.

   Let F be a finite field of characteristic p. Show that F contains p^n elements for some n. Show also that the map

   $$\Phi : x \mapsto x^p$$

   is an automorphism of F; and show that every automorphism of F is of the form $x \mapsto \Phi^i(x)$ for some i.

10. Show that the prime (irreducible) factors of the polynomial

$$x^{p^n} - x$$

over $\mathbf{GF}(p)$ are precisely the prime polynomials over $\mathbf{GF}(p)$ whose degree d divides n.

Hence show that if there are $\Pi(n) = \Pi_p(n)$ prime polynomials of degree n over $\mathbf{GF}(p)$, then

$$\sum_{d|n} d\Pi(d) = p^n$$

for each positive integer n.

Determine all prime polynomials of degree 5 over $\mathbf{GF}(2)$.

Explain what is meant by saying that a prime polynomial over $\mathbf{GF}(p)$ is *primitive*. Show that there are

$$\frac{1}{n}\phi\left(p^n - 1\right)$$

primitive polynomials of degree n over $\mathbf{GF}(p)$, where ϕ is Euler's function.

Determine which of the prime polynomials of degree 5 over $\mathbf{GF}(2)$ are primitive.