UNIVERSITY OF ABERDEEN **SESSION 2004–05**

DEGREE EXAMINATION

MX4033 Number Theory

Friday 21 January 2005 (3pm to 5pm)

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 THREE questions. All questions carry equal weight.

1. **(a)** Let p be an odd prime number, a an integer not divisible by p. Define the *Legendre symbol*

$$\left(\frac{a}{p}\right).$$

Define what is meant by a *quadratic residue* modulo p and a *quadratic non-residue* modulo p. Show that exactly half of the elements of $(\mathbb{Z}/p)^*$ are quadratic residues modulo p.

Prove Euler's criterion:

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \mod p.$$

State the quadratic reciprocity law.

(b) Let p be a prime number which is congruent to 5 modulo 12. Show that $3^{(p-1)/2} \equiv -1 \mod p$.

Let p be a prime number which has the form $2^k + 1$ for some integer $k > 0$. Let a be an integer not divisible by p. Show that if

$$\left(\frac{a}{p}\right) = -1\,,$$

then $[a]$ is a generator for the group $(\mathbb{Z}/p)^*$.

Let $m = 2^k + 1$, where $k > 0$ is an even integer. Show that m is prime if and only if

$$3^{(m-1)/2} \equiv -1 \mod m\,.$$

2. **(a)** Let $f(x)$ be a polynomial with integer coefficients. Prove that

$$f(a+h) \equiv f(a) + f'(a)h \mod h^2$$

for any $a, h \in \mathbb{Z}$.

Suppose in addition that $f(a) \equiv 0 \mod p^k$ and $f'(a) \not\equiv 0 \mod p$, where p is a prime and $k > 0$ is an integer. Show that the pair of congruences

$$f(x) \equiv 0 \mod p^{k+1} , \qquad x \equiv a \mod p^k$$

has an integer solution, unique modulo p^{k+1}.

Hence show that the congruence $x^{p-1} \equiv 1 \mod p^k$ (for a prime p and an integer $k > 0$) has exactly $p-1$ solutions, counted modulo p^k.

Find an integer solution for the congruence $x^4 + 2x + 4 \equiv 0 \mod 27$.

(b) In the congruence

$$ax^2 + bx + c \equiv 0 \mod p ,$$

suppose that p is an odd prime, $a, b, c \in \mathbb{Z}$, and p does not divide a. Let $D = b^2 - 4ac$. Prove that the congruence has: no integer solutions if D is a quadratic non-residue mod p ; a unique solution modulo p if p divides D ; exactly two solutions modulo p if D is a quadratic residue modulo p.

3. Show that the polynomial $W(x) = x^3 - x + 1$ is irreducible in $\mathbb{Q}[x]$.

Let $\gamma \in \mathbb{C}$ be a root of $W(x)$. Define what is meant by $\mathbb{Q}[\gamma]$. Explain why $K = \mathbb{Q}[\gamma]$ is a field. Explain how K can be regarded as a vector space over $\mathbb{Q}$. Show that $1, \gamma, \gamma^2$ constitute a basis for K (as a vector space over $\mathbb{Q}$).

Define what is meant by the *field polynomial*, the *norm* and the *trace* of an element in K. [If your definition refers to a specific basis of K as a vector space over $\mathbb{Q}$, show that another choice of basis will give the same results.] Calculate the trace of an element $a+b\gamma+c\gamma^2 \in K$, where $a, b, c \in \mathbb{Q}$. [Express it in terms of a, b and c.]

Define what is meant by the *discriminant* of K with respect to a vector space basis of K. Calculate the discriminant of K with respect to the basis $1, \gamma, \gamma^2$.

Hence determine $\mathcal{O}_K$, the ring of algebraic integers in K. [Determine what $a, b, c \in \mathbb{Q}$ must satisfy so that $a + b\gamma + c\gamma^2$ is an algebraic integer.]

4. **(a)** Describe the roots of $x^5 - 1$ in $\mathbb{C}$.

State Eisenstein's criterion for irreducibility in $\mathbb{Q}[x]$. [You are not required to prove it.]

Decompose $x^5 - 1$ into irreducible factors in $\mathbb{Q}[x]$.

Let $K = \mathbb{Q}[\xi]$ where ξ is any root of $x^5 - 1$, but $\xi \neq 1$. Show that the dimension of K as a vector space over $\mathbb{Q}$ is 4.

Define what is meant by an *algebraic integer*.

The ring $\mathcal{O}_K$ of algebraic integers in K is precisely $\mathbb{Z}[\xi]$. [You are not required to prove this and you may use it in the following.] Determine the factorization of the ideal $5\mathcal{O}_K$ into prime ideals, stating any general results that you may be using. [*Hint*: at some point you may want to use $(a+b)^5 = a^5 + b^5$ for a, b in the field $\mathbb{Z}/5$.]

(b) Describe the ring $\mathcal{O}_L$ of algebraic integers in the field $L = \mathbb{Q}[\sqrt{5}]$, stating carefully any result from the lectures that you are using.

Show that if p is a prime number which is congruent to ± 1 mod 5, then $p\mathcal{O}_L$ is not a prime ideal in $\mathcal{O}_L$.