UNIVERSITY OF CAMBRIDGE

MATHEMATICAL TRIPOS Part III

Tuesday 6 June, 2006 1.30 to 3.30

PAPER 27

TOPICS IN NUMBER THEORY

*Attempt **THREE** questions.*

*There are **FOUR** questions in total.*

The questions carry equal weight.

Throughout, p denotes a prime number.

STATIONERY REQUIREMENTS
Cover sheet
Treasury Tag
Script paper

SPECIAL REQUIREMENTS
None

You may not start to read the questions printed on the subsequent pages until instructed to do so by the Invigilator.

1

(i) Prove that the multiplicative group of $\mathbb{Q}_p$ is isomorphic to $\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p \times \mathbb{Z}$ if $p \neq 2$.

(ii) Let K be complete with respect to a nonarchimedean absolute value, with residue field k_K. What does it mean to say that a finite extension L/K is *unramified*? Show that if L/K is unramified then $\mathfrak{o}_L = \mathfrak{o}_K[x]$ for any $x \in \mathfrak{o}_L$ whose reduction $\bar{x}$ modulo the maximal ideal satisfies $k_L = k_K[\bar{x}]$.

2

(i) State carefully Mahler's theorem. Show that the Mahler coefficients of a continuous function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ are given by the generating function

$$\sum_{n\geq 0} \frac{c_n}{n!} T^n = e^{-T} \sum_{n\geq 0} \frac{f(n)}{n!} T^n.$$

(ii) Show that if $f : \mathbb{Z}_p \to \mathbb{Z}_p$ is continuous, then the function $g : \mathbb{N} \to \mathbb{Z}_p$ defined by

$$g(n) = f(0) + \ldots + f(n-1), \quad g(0) = 0$$

extends to a continuous function $\mathbb{Z}_p \to \mathbb{Z}_p$. What is its Mahler expansion?

(iii) Show that any linear form $L : \mathcal{C}(\mathbb{Z}_p, \mathbb{Q}_p) \to \mathbb{Q}_p$ which is invariant under translations (i.e. if $h(x) = f(x+a)$ for some $a \in \mathbb{Z}_p$ then $L(f) = L(h)$) is zero.

3 Let K be a field of characteristic zero, complete with respect to a discrete valuation, with valuation ring $\mathfrak{o}_K$ and uniformiser π. Let $f(X) \in \mathfrak{o}_K[X]$ and $x \in \mathfrak{o}_K$ such that $f(x) \equiv 0 \pmod{\pi}$ and $f'(x) \not\equiv 0 \pmod{\pi}$. Show that there exists a unique $y \in \mathfrak{o}_K$ such that $x \equiv y \pmod{\pi}$ and $f(y) = 0$.

Suppose that the residue field of K is finite, of order $q = p^r$. Show that the group of roots of unity of K has order $p^s(q-1)$ for some $s \geq 0$. Show that if $v(p) < p-1$ (where the valuation is normalised so that $v(\pi) = 1$) then $s = 0$. Show by example that if $v(p) = p-1$ both $s = 0$ and $s = 1$ can occur.

4

(i) Let K be a field and $|\cdot|$ a nonarchimedean absolute value on K, with associated valuation ring $\mathfrak{o}$. Show that $\mathfrak{o}$ is a local ring which is integrally closed. Show also that $\mathfrak{o}$ is a principal ideal domain if and only if the valuation associated to $|\cdot|$ is discrete.

(ii) State and prove Krasner's lemma.

(iii) By considering the series $\sum_{n\geq 0} p^n \zeta_{p^{n+1}}$ or otherwise, show that the algebraic closure of $\mathbb{Q}_p$ is not complete.

END OF PAPER