M381/T

The Open University

Third Level Course Examination 1997

Number Theory and Mathematical Logic

Thursday, 23 October, 1997 10.00 am – 1.00 pm

Time allowed: 3 hours

This paper is in two Parts. Part I (Questions 1–8) is on Number Theory and Part II (Questions 9–16) is on Mathematical Logic.

Your examination grade will be the sum of your best **NINE** question scores, where *not more than six* of these come from a single Part.

If you exceed six questions from one Part, all questions will be marked but credit will be given only for your best **NINE** questions within the restriction stated above. You may cross out any work that you do not wish the examiner to mark.

Use a **separate** answer book for **each** part.

All questions carry equal marks. The allocation of marks within a question is indicated by a number in brackets, [ ], beside the question.

At the end of the examination

Check that you have written your name, personal identifier and examination number on each answer book used. **Failure to do so will mean that your work cannot be identified.** Attach all your answer books together using the fastener provided.

The use of calculators is not permitted in this examination

Answer as many questions as you wish. Full marks may be obtained by **complete** *answers to* **NINE** *questions, provided that no more than* **SIX** *questions have been selected from any one part. All questions carry equal marks.*

PART I NUMBER THEORY

Question 1

(i) Use the Euclidean Algorithm to determine the greatest common divisor of 161 and 253, and hence find integers x and y such that

$$\gcd(161, 253) = 161x + 253y. \qquad [3]$$

(ii) The Fibonacci sequence is defined by

$$F_1 = F_2 = 1; \quad F_{n+2} = F_{n+1} + F_n, \quad \text{for } n \geq 1.$$

Use Mathematical Induction to prove that

$$F_1 + 2F_2 + 3F_3 + \cdots + nF_n = (n+1)F_{n+2} - F_{n+4} + 2$$

for all $n \geq 1$. [5]

(iii) Prove Euclid's Lemma, namely that if a, b and c are integers such that $a|bc$ with $\gcd(a, b) = 1$, then $a|c$. [You may assume, without proof, any other result given in the Handbook entry for Unit 1.] [3]

Question 2

For each of the following statements about integers k, m and n, decide whether it is true or false. If true, prove it: if false, justify your answer.

(i) Any number of the form $6k + 1$, where $k \geq 1$, must have a prime divisor of this same form.

(ii) Any number of the form $6k + 5$, where $k \geq 0$, must have a prime divisor of this same form.

(iii) If $\gcd(m, n) = 1$ then $\gcd(6m + 1, 6n + 1) = 1$.

(iv) There are infinitely primes of the form $6k + 5$. [11]

Question 3

(i) Prove, from the definition of congruence alone, that if $na \equiv nb \pmod{mn}$ then $a \equiv b \pmod{m}$, where a, b, m and n are integers, with m and n positive. Use this result in solving the linear congruence

$$48x \equiv 12 \pmod{150}. \qquad [5]$$

(ii) Solve the polynomial congruence $x^3 - 2x - 4 \equiv 0 \pmod{5}$. [2]

(iii) Find the least positive integer which satisfies each of the following linear congruences simultaneously:

$$x \equiv 1 \pmod{3}; \quad x \equiv 2 \pmod{5}; \quad x \equiv 2 \pmod{11}. \qquad [4]$$

Question 4

(i) Use Fermat's Little Theorem (FLT) to show that $3^{100} - 2^{100}$ is divisible by 13. [4]

(ii) Determine the smallest prime divisor of $16! + 1$. [3]

(iii) Find the least positive remainder when 24^{24} is divided by 77. [Note that 77 is not prime.] [4]

Question 5

(i) Prove that every number of the form $2^{k-1}(2^k - 1)$, where $2^k - 1$ is prime (k an integer with $k \geq 2$), is perfect. [3]

(ii) A positive integer n has the property that $n + 2\phi(n)$ is divisible by 3 (where ϕ is Euler's phi-function).

(a) Prove that n cannot be prime.

(b) Determine for which primes p, if any, $n = p^2$.

(c) If $n = pq$, where $p > 3$ and $q > 3$ are distinct primes, prove that $p \equiv q \equiv 2 \pmod 3$. [8]

Question 6

(i) Determine whether or not the quadratic congruence

$$3x^2 + 6x - 2 \equiv 0 \pmod{47}$$

has solutions. [4]

(ii) Evaluate the Legendre symbol $(-39/67)$. [3]

(iii) Use the Law of Quadratic Reciprocity (LQR) to prove that for an odd prime $p \neq 3$,

$$(3/p) = \begin{cases} 1, & \text{if } p \equiv \pm 1 \pmod{12}, \\ -1, & \text{if } p \equiv \pm 5 \pmod{12}. \end{cases}$$ [4]

Question 7

(i) Determine a simple finite continued fraction for $57/32$ and hence find the solution of the linear Diophantine equation

$$57x - 32y = 1$$

in which y takes its least positive value. [5]

(ii) Determine the irrational number α whose continued fraction is $[0, 1, \langle 1, 2 \rangle]$. Write down the convergents C_1, C_2, C_3, C_4, C_5 and C_6 of α and indicate (with brief justification) which is the first convergent accurate to within 0.01 as an approximation to α. [6]

Question 8

(i) Given that the continued fraction of $\sqrt{11}$ is $[3, \langle 3, 6 \rangle]$, determine two positive solutions of the Diophantine equation

$$x^2 - 11y^2 = 1.$$ [4]

(ii) Determine two Pythagorean triples, one which is primitive and one which is not, in which one of the sides is 20. [3]

(iii) Use the method of infinite descent to prove that the Diophantine equation

$$x^3 - 4y^3 = 2z^3$$

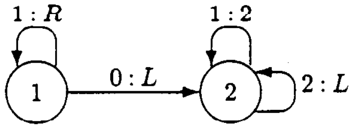
has no solution in positive integers. [4]

PART II MATHEMATICAL LOGIC

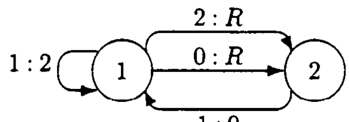
Question 9

(i) We wish to design a Turing machine which, if started scanning the leftmost of a string of n 1s (on an otherwise blank tape), would halt scanning a single 2 on an otherwise blank tape.

(a) Explain why each of the Turing machines below is *not* suitable for this task. (Your answer may include sequences of configurations for appropriate test data.)



(1)



(2)

[4]

(b) Give the flowgraph of a machine which correctly performs the task. [2]

(ii) Give the complete flowchart of an Abacus machine program which has the effect shown in the following block diagram. (You may use extra registers, assumed empty initially, if you wish.)

$$\begin{array}{c}\downarrow\\ \boxed{\begin{array}{r}\mathrm{Max}([m],[n]) \longrightarrow p\\ |[m]-[n]| \longrightarrow n\\ 0 \longrightarrow m\end{array}}\\ \downarrow\end{array} \quad \text{where } \mathrm{Max}(x,y) = \begin{cases} y, & \text{if } y \geq x,\\ x, & \text{if } y < x,\end{cases}$$

$$\text{and } |x-y| = \begin{cases} y-x, & \text{if } y \geq x\\ x-y, & \text{if } y < x.\end{cases}$$

where $[p] = 0$ initially.

[5]

Question 10

(i) Let h be the function

$$\mathrm{Pr}[s, \mathrm{Cn}[\mathrm{prod}, \mathrm{Cn}[s, \mathrm{id}^3_3], \mathrm{Cn}[s, \mathrm{id}^3_2]]]$$

where prod is the product function defined by $\mathrm{prod}(x, y) = x \cdot y$.

Compute the values of

(a) $h(4, 0)$,

(b) $h(4, 2)$. [4]

(ii) In this part you may present your arguments using either formal or informal definitions.

(a) Show that the function prod, as in part (i), is primitive recursive by defining it in terms of the initial functions. [2]

(b) Show that the function f of 3 arguments defined by

$$f(x_1, x_2, x_3) = (x_1 \cdot x_2)^{x_3}$$

is primitive recursive by defining it in terms of the initial functions and, if you wish, the sum and product functions. [2]

(iii) Write down the pairs (x_1, x_2) of natural numbers for which $\mathrm{Mn}[f](x_1, x_2)$ is defined, where f is the function defined by

$$f(x_1, x_2, y) = x_1^{y+1} \cdot ((x_2 + y) \dot{-} x_1).$$

[3]

Question 11

(i) A Turing machine has a configuration with left number 29 and right number 54. Draw the configuration which results when the scanning head has moved one square to the left, and find its left and right numbers. [3]

(ii) In parts (a), (b) and (c) below, you may use any of the recursive functions, or results about them, given in the Logic Handbook without proving that they are recursive. You may give your answers as informal definitions.

(a) Show that the condition "$y \geq x$" on pairs (x, y) of natural numbers is primitive recursive. [3]

(b) Show that the function Max defined by

$$\text{Max}(x, y) = \begin{cases} y, & \text{if } y \geq x, \\ x, & \text{if } y < x, \end{cases}$$

is primitive recursive. [$1\frac{1}{2}$]

(c) Show that the function f defined by

$$f(x_1, x_2, x_3) = \begin{cases} x_1^{x_2}, & \text{Max}(x_1, x_3) \geq x_2 + 21, \\ 7, & \text{if } 3x_1 + 4x_2 + 5x_3 = 60, \\ 3x_3, & \text{otherwise,} \end{cases}$$

is primitive recursive. [$3\frac{1}{2}$]

Question 12

In this question, with the exception of the proviso given in part (i), you may use any of the recursive functions, or results about them, given in the Logic Handbook without proving that they are recursive. You may also give your answers as formal or informal definitions.

(i) Prove that if f is a primitive recursive function of 2 arguments, then the function h defined by

$$h(x, y) = \sum_{z=0}^{y} f(x, z)$$

is also primitive recursive. You may *not* use the result in the Handbook of which this is a special case. [3]

(ii) By summing the values of $d(x, y)$ for appropriate values of y, where the function d (given as primitive recursive in the Logic Handbook) is defined by

$$d(x, y) = \begin{cases} 1, & \text{if } x \text{ is divisible by } y, \\ 0, & \text{otherwise,} \end{cases}$$

show that the function p defined by

$$p(x) = \begin{cases} 1, & \text{if } x \text{ is a prime number,} \\ 0, & \text{otherwise,} \end{cases}$$

is primitive recursive. [5]

(iii) Show that the function t defined by

$$t(x) = \begin{cases} 1, & \text{if } x \text{ and } x + 2 \text{ are both prime,} \\ 0, & \text{otherwise,} \end{cases}$$

is primitive recursive. [3]

Question 13

(i) Show that the following formula takes truth value 1 under all interpretations of its symbols.

$$(((x = 0 \vee \forall x\, x = 0) \rightarrow \forall x(x = 0 \vee \forall x\, x = 0)) \rightarrow (-\forall x(x = 0 \vee \forall x\, x = 0) \rightarrow -x = 0)) \qquad [3]$$

(ii) The following is a correct (but contorted) proof from which the assumption numbers have been omitted.

(1)	$(\psi \rightarrow \theta)$	Ass
(2)	$\forall x(\theta \,\&\, \phi)$	Ass
(3)	$(\theta \,\&\, \phi)$	UE, (2)
(4)	$\exists x(\psi \rightarrow \theta)$	Ass
(5)	$(\psi \rightarrow \theta)$	Taut, (1), (3)
(6)	$\exists x(\psi \rightarrow \theta)$	EI, (5)
(7)	$\exists x(\psi \rightarrow \theta)$	EH, (6)
(8)	$((\psi \rightarrow \theta) \rightarrow \exists x(\psi \rightarrow \theta))$	CP, (6)
(9)	$((\psi \rightarrow \theta) \rightarrow \exists x(\psi \rightarrow \theta))$	Taut, (7)

(a) Write down the assumptions in force on each line. $[2\frac{1}{2}]$

(b) Write down the tautology used on line (9). $[\frac{1}{2}]$

(c) For each of the following lines, write down whether the proof would still be correct were the line to be added to it.

(A)	1 (10)	$\forall x(\psi \rightarrow \theta)$	UI, (1)
(B)	4 (10)	$(\psi \rightarrow \theta)$	EH, (1)

Answer YES or NO. [2]

(iii) (a) Give an example of formulas ϕ and θ for which θ is a tautological consequence of ϕ. $[1\frac{1}{2}]$

(b) Give an example of formulas ϕ and θ for which θ is a logical, but not a tautological, consequence of ϕ. $[1\frac{1}{2}]$

(No justification is required in either case.)

Question 14

(i) Which of the following terms are freely substitutable for x in the formula

$$\forall t(\exists z(x + y) = z \rightarrow \exists y \forall x(x + t) = y)?$$

(a) $(x \cdot 0)'$

(b) $(x + t)$

(c) $(x + y)$

Answer YES or NO in each case. [2]

(ii) Give formal proofs to show each of the following results.

(a) $\exists x \forall y(x + y) = y \vdash \forall y \exists x(x + y) = y$ [3]

(b) $\forall x(-\phi \vee -\psi) \vdash (\psi \rightarrow -\exists x(\phi \,\&\, \theta))$, where the variable x does not occur free in ψ. Indicate the step(s) of your proof which require the condition on ψ. [6]

Question 15

For each of the following sentences, decide whether or not it is a theorem of Q. If it is a theorem of Q, write down a formal proof showing this. If it is not a theorem of Q, justify this. (*You may use without proof the fact that all the axioms of Q are true under the interpretations N^* and N^{**} given in the Logic Handbook.*)

(i) $\forall x((\mathbf{0} \cdot \mathbf{0}) \cdot x) = ((\mathbf{0} \cdot x)) + (x \cdot \mathbf{0}))$

(ii) $\forall x \forall y(x' \cdot y) = ((x \cdot y) + y)$

(iii) $\forall x \exists y(x' \cdot y) = (y' \cdot x)$ [11]

Question 16

(i) Explain briefly what is meant by Church's Thesis, what evidence there is for it to be true and what would be needed to show it false. [3]

(ii) Give brief explanations of *each* of the following:

(a) a *decidable* theory;

(b) the theory *arithmetic*. [3]

(iii) Is the theory Z (of Elementary Peano Arithmetic) decidable? Briefly explain your answer. [2]

(iv) Which theorem (or theorems) of the course give(s) an answer to Leibniz's Question:

> *Is there an algorithm for deciding which statements of number theory are true?*

Explain why the theorem(s) answer(s) the question. In particular, what roles, if any, do Church's Thesis and the theory arithmetic play in answering the question? [3]

(*Your answer may include references to any of the theorems listed in the Logic Handbook.*)

[END OF QUESTION PAPER]

M381/T ERRATA

Page 2, Question 2 (iv)

"infinitely primes" should be "infinitely many primes".

Page 5, Question 11 (ii)(c)

There should be the word "if" in front of "Max(x_1,x_3)...".

Page 7, Question 15 (i)

A superfluous bracket on the righthand side of the equality should be removed, so that the expression reads as "$((\mathbf{0} \cdot x) + (x \cdot \mathbf{0}))$".