M381/E

The Open University

Third Level Course Examination 1998

Number Theory and Mathematical Logic

Wednesday 14 October 1998 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 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 87 and 126, and hence find positive integers x and y such that

$$\gcd(87, 126) = 87x - 126y.$$ [4]

(ii) Use Mathematical Induction to prove that the formula

$$1 + 5 + 12 + 22 + \cdots + \tfrac{1}{2}n(3n-1) = \tfrac{1}{2}n^2(n+1)$$

holds for all integers $n \geq 1$. [4]

(iii) Suppose that m and n are positive integers such that n has remainder 3 when divided by 4, and $m = 7n + 4$. Prove that $\gcd(m, n) = 1$. [3]

Question 2

(i) If integers $p_1, p_2, \ldots, p_r$ are all of the form $3k + 2$, where k is an integer, prove that $(p_1 p_2 \ldots p_r)^2$ is of the form $3k + 1$. [3]

(ii) Prove that any positive number of the form $3k + 2$ must have a prime divisor of this same form. [3]

(iii) Prove that there are infinitely many primes of the form $3k + 2$ by the following method. Suppose that $p_1, p_2, \ldots, p_r$ are all the primes of the form $3k + 2$. Construct from this list of primes a number of the form $3k + 2$ which is not divisible by any prime in this list and explain why this proves the assertion. [5]

Question 3

(i) Suppose that $n \equiv 4 \pmod 6$. Find the least positive residue of $12n + 5$

(a) modulo 8;

(b) modulo 9. [2]

(ii) Let p be an odd prime and a be such that $\gcd(a, p) = 1$. Prove that

$$2,\ 2 + a,\ 2 + 2a,\ 2 + 3a, \ldots,\ 2 + (p-1)a$$

forms a complete set of residues modulo p. [3]

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

$$x \equiv 1 \pmod 3; \quad x \equiv 2 \pmod 5; \quad 3x \equiv 5 \pmod{11}.$$ [6]

(i) Use Fermat's Little Theorem (FLT):

(a) to determine the remainder when $5^{50} + 3^{30}$ is divided by 13;

(b) to prove that

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$$

where p and q are distinct primes. [6]

(ii) You are given that the recurring decimal of $1/19$ is

$$1/19 = 0.\langle 052631578947368421 \rangle.$$

Answer the following, in each case giving brief justification of your answer.

(a) What is the order of 10 modulo 19?

(b) What is the value of 10^9 modulo 19?

(c) Write down the recurring decimal of $\frac{12}{19}$. [5]

Question 5

This question is concerned with the multiplicative functions σ and ϕ, where σ denotes the 'sum of the divisors' function and ϕ is Euler's ϕ-function.

(i) An integer n with $\sigma(n) > 2n$ is said to be an *abundant* number.

(a) Is 74 abundant?

(b) Is 174 abundant?

(c) For which primes p is $10p$ abundant? [7]

(ii) Show that if p and $2p - 1$ are both odd primes then $\phi(4p) = \phi(4p - 2)$. [4]

Question 6

(i) Determine whether or not the quadratic congruence

$$2x^2 - 5x + 4 \equiv 0 \pmod{37}$$

has solutions. [3]

(ii) Evaluate the Legendre symbol $(67/107)$. [3]

(iii) Determine all primes $p > 3$ for which

$$(6/p) = 1.$$

[You may use results given in the Handbook relating to $(2/p)$ and $(3/p)$ if you so wish.] [5]

Question 7

(i) Determine the two simple finite continued fractions for $\frac{39}{14}$. [2]

(ii) Determine the irrational number whose continued fraction is $[2, \langle 3, 1 \rangle]$. [4]

(iii) Determine the infinite simple continued fraction for $\frac{\sqrt{5}}{2}$. [5]

Question 8

(i) Determine all primitive Pythagorean triples (if any) in which one of the sides is

(a) 14;

(b) 16. [4]

(ii) Of the two numbers 610 and 620 one can be written as a sum of two squares while the other cannot. Explain why the one cannot be expressed in this way and write the other as a sum of two squares. [3]

(iii) Suppose that $\sqrt{7} = \frac{m}{n}$, where m and n are positive integers. Deduce that

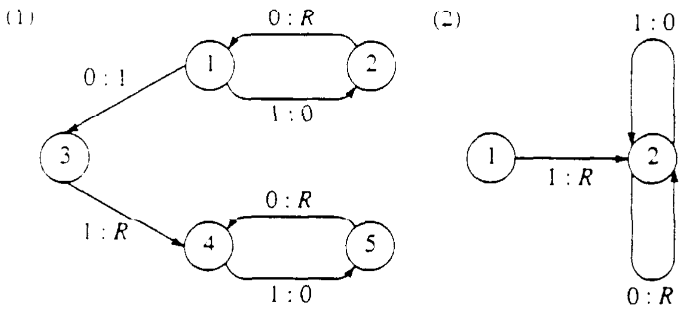
$$\sqrt{7} = \frac{7n - 2m}{m - 2n}$$

and show how the method of infinite descent can be used to deduce from this that $\sqrt{7}$ is irrational. [4]

Question 9

(i) We wish to design a Turing machine which, using monadic notation, takes as input a pair (m, n) of positive integers in standard position (on an otherwise blank tape) and which halts scanning a single 1 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.)



[4]

(b) Give the flowgraph of a Turing 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.)

$$\begin{array}{|rl|} \hline [m] \dot{-} [n] & \longrightarrow p \\ \mathrm{Min}([m],[n]) & \longrightarrow m \\ 0 & \longrightarrow n \\ \hline \end{array}$$

where $[p] = 0$ initially.

$$\text{where } x \dot{-} y = \begin{cases} x - y, & \text{if } x \geq y, \\ 0, & \text{if } x < y, \end{cases}$$

$$\text{and } \mathrm{Min}(x, y) = \begin{cases} y, & \text{if } x \geq y, \\ x, & \text{if } x < y. \end{cases}$$

[5]

Question 10

(i) Let h be the function

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

where exp is the function defined by $\exp(x, y) = x^y$.

Compute the values of

(a) $h(2, 0)$,

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

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

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

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

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

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

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

$$f(x_1, x_2, y) = (x_2 \dot{-} (y + x_1)) + (x_1 \dot{-} 7) \cdot y?$$ [3]

Question 11

(i) A Turing machine has a configuration with left number 41 and right number 91. Draw the configuration which results when the scanning head has moved one square to the right, and find its left and right numbers. [3]

(ii) In parts (a), (b) and (c) below, you may use any of the recursive functions except e, Eq and d, or results about recursive functions, given in the Logic Handbook without proving that they are recursive.

(a) Show that the condition "$x = y$" on pairs (x, y) of natural numbers is primitive recursive. [$2\frac{1}{2}$]

(b) Show that the condition "x is even" on natural numbers x is primitive recursive. [2]

(c) Show that the function f defined by

$$f(x, y) = \begin{cases} x^{3y}, & \text{if } x \cdot y + 4 \text{ is odd,} \\ y, & \text{if } 2x + 3y = 8000, \\ 2, & \text{otherwise,} \end{cases}$$

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

Question 1[illegible]

In this question 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 informal definitions.

(i) Show that the function c defined by

$$c(x,y) = \begin{cases} 1, & \text{if } y^2 \leq x, \\ 0, & \text{otherwise}, \end{cases}$$

is primitive recursive. [3]

(ii) Show that if f is primitive recursive function of 2 arguments, then the function g defined by

$$g(x,v,w) = \begin{cases} \sum_{z=v}^{w} f(x,z), & \text{if } w \geq v, \\ 0, & \text{if } w < v, \end{cases}$$

is also primitive recursive. [3]

(iii) By summing the values of $c(x,z)$ for appropriate values of z, or otherwise, show that the function k defined by

$$k(x) = \left[x^{1/2}\right],$$

i.e. the greatest integer less than or equal to the square root of x (so that e.g. $k(0) = 0$, $k(1) = k(2) = k(3) = 1$, $k(4) = \cdots = k(8) = 2$, $k(9) = 3$) is primitive recursive. [4]

(iv) Explain briefly how to adapt the above argument to show that the function j defined by

$$j(x) = [x^{1/4}],$$

i.e. the greatest integer less than or equal to the fourth root of x, is primitive recursive. [1]

Question 13

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

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

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

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

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

(b) Write down the tautology used on line (7). [$\frac{1}{2}$]

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

(A)	2	(10) $\exists x(\theta \vee \phi)$	EI, (4)
(B)	2	(10) $\forall x(\theta \vee \phi)$	UI, (4)

Answer YES or NO. [2]

(iii) By giving an example from everyday maths along with a relevant rule of proof (in the Logic Handbook), explain why the validity of the rule you have chosen requires a variable not to occur free in some of the formulas mentioned within the statement of that rule. [3]

Question 14

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

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

(a) $(t + z)$

(b) $(x \cdot t)$

(c) $(x + y)$

Answer YES or NO in each case. [2]

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

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

(b) $\phi \vdash (\forall x(\psi \vee -\phi) \rightarrow -\exists x -(\theta \rightarrow \psi))$ where the variable x does not occur free in ϕ. Indicate the step(s) of your proof which require the condition on ϕ. [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) $\forall x(0 + (x \cdot 0)) = ((0 + x) \cdot 0)$

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

(iii) $\exists x -(x + x) = (x + x)''$ [11]

Question 16

(i) Explain briefly what is meant by saying that the theory Z (of Elementary Peano Arithmetic) is *consistent*. [2]

(ii) (a) Give a formal proof in the theory Z to show that

$$\vdash_Z \neg 0 = 1.$$ [2]

(b) Deduce that if Z is consistent then $\mathbf{0} = \mathbf{1}$ is not a theorem of Z. [1]

(iii) Explain briefly when the formula $\text{Prov}(y)$ is true in the standard interpretation. [2]

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

Can the consistency of number theory be proved using only non-dubious principles of finitary reasoning?

Explain why the theorem(s) answer(s) the question.

(*Your answer may include references to any of the theorems listed in the Logic Handbook.*) [4]

[END OF QUESTION PAPER]