M381/G

The Open University

Third Level Course Examination 1999

Number Theory and Mathematical Logic

Wednesday 14 October 1999 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 91 and 156, and hence write down the general solution of the linear Diophantine equation

$$\gcd(91, 156) = 91x + 156y. \qquad [4]$$

(ii) Prove that for any integer n, $\gcd(6n - 1, 6n + 3) = 1$. [3]

(iii) Use Mathematical Induction to prove that, for all positive integers n,

3^{3n} has remainder 1 when divided by 13. [4]

Question 2

For each of the following statements, decide whether it is true or false. If it is true, prove it. If you claim it to be false, justify your answer.

(i) There are infinitely many primes.

(ii) Any number of the form $17k + 2$, where $k \geq 0$ is a non-negative integer, must have a prime divisor of this same form.

(iii) If a, b and c are positive integers such that

$a^2 + b^2 + c^2$ is divisible by 5,

then at least one of a, b or c is divisible by 5. [11]

Question 3

(i) Suppose that $n \equiv 5 \pmod 8$. Find the least positive residue of $6n + 3$

(a) modulo 8;

(b) modulo 12. [2]

(ii) Prove that, for any integers a, b, $r \neq 0$ and $n \geq 2$

$ra \equiv rb \pmod{rn}$ if and only if $a \equiv b \pmod n$. [3]

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

$$x \equiv 2 \pmod 3; \quad 2x \equiv 1 \pmod 7; \quad 6x \equiv 8 \pmod{11} \qquad [6]$$

Question 4

(i) Prove Wilson's Theorem: if p is prime then $(p - 1)! \equiv -1 \pmod p$. [5]

(ii) Use Fermat's Little Theorem (FLT) or its Corollary:

(a) to find the least positive residue of 7^{100} modulo 17;

(b) to show that $a^{13} \equiv a \pmod{105}$ for all integers a.
[Note that 105 is not prime.] [6]

Question 5

Both parts of this question involve the function $\sigma(n)$, which gives the sum of the positive divisors of n.

(i) Suppose that p is prime. Prove that $m = 2^{p-1}(2^p - 1)$ is perfect if and only if $2^p - 1$ is prime. [4]

(ii) Suppose that the integer n has the property that $n + 2\sigma(n)$ is divisible by 3.

(a) Show that n cannot be prime.

(b) Show that if $n = p^2$, where p is prime, then $p \equiv 2 \pmod 3$;

(c) For which primes p is $n = 2p$ possible? Justify your answer. [7]

Question 6

(i) Determine whether or not the quadratic congruence

$$3x^2 + 4x + 5 \equiv 0 \pmod{17}$$

has solutions. [3]

(ii) Evaluate the Legendre symbol (127/167). [Note that both 127 and 167 are prime.] [4]

(iii) Use Gauss' Lemma to prove that 2 is a quadratic residue of any prime p of the form $8k + 7$. [4]

Question 7

(i) Determine a simple finite continued fraction for 55/42 and, from it, find a solution of the Diophantine equation

$$42x - 55y = 1$$

in which x and y are each positive. [5]

(ii) Determine the irrational number which has the periodic continued fraction

$$[2, 2, \langle 1, 2\rangle].$$ [6]

Question 8

(i) Given that the infinite continued fraction of $\sqrt{8}$ is $[2, \langle 1, 4\rangle]$, write down three positive solutions of Pell's equation

$$x^2 - 8y^2 = 1.$$ [4]

(ii) Of the two numbers 980 and 990, one can be written as a sum of two squares while the other cannot. Explain why the one cannot be expressed this way and write the other as a sum of two squares. [3]

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

$$x^3 + 3y^3 = 9z^3$$

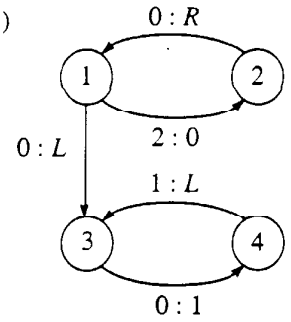
has no solution in positive integers. [4]

Question 9

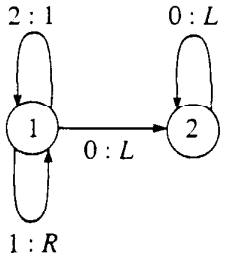
(i) We wish to design a Turing machine which, if started scanning the leftmost of a string of n 2s (on an otherwise blank tape), would halt scanning the leftmost of a string of n 1s on an otherwise blank tape.

(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)



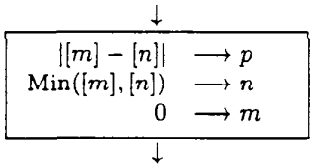
(2)



[4]

(b) Give the flowgraph of a 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.)



where $[p] = 0$ initially.

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

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

[5]

Question 10

(i) Let h be the function

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

where dif is the function defined by $\mathrm{dif}(x,y) = \begin{cases} x-y, & \text{if } x \geq y, \\ 0, & \text{if } x < y. \end{cases}$

Compute the values of

(a) $h(3,0)$,

(b) $h(3,2)$. [4]

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

(a) Show that the product function is primitive recursive by defining it in terms of the initial functions. [3]

(b) Show that the function

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

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

$$f(x_1,x_2,y) = x_2^{y+1} \cdot ((x_1+y) \dot{-} x_2).$$ [2]

Question 11

(i) A Turing machine has a configuration with left number 25 and right number 54. Draw the configuration which results when the scanning head has moved one square to the left, and write down the new left and right numbers. [3]

(ii) In parts (a), (b) and (c) below, subject to the given proviso in (a) 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 if g_1, g_2 and g_3 are primitive recursive functions and C_1 and C_2 are mutually exclusive primitive recursive conditions on pairs (x,y) of natural numbers, then the function f defined by

$$f(x,y) = \begin{cases} g_1(x,y), & \text{if } C_1, \\ g_2(x,y), & \text{if } C_2, \\ g_3(x,y), & \text{otherwise,} \end{cases}$$

is primitive recursive. You may *not* use either of the results on page 3 of the Logic Handbook of which this is a special case. [2½]

(b) Prove that if C_1 and C_2 are both primitive recursive conditions on pairs (x,y) of natural numbers, then so is the condition "C_1 and C_2". [2]

(c) Show that the function f defined by

$$f(x,y) = \begin{cases} 3xy, & \text{if } 5x+7y \text{ is even,} \\ y^4, & \text{if } x \text{ is odd and } 2x = y, \\ 5, & \text{otherwise,} \end{cases}$$

is primitive recursive. [3½]

Question 12

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

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

is primitive recursive. [3]

(ii) Given two natural numbers x, y with $y \neq 0$, there exist unique natural numbers q and r such that

$$x = qy + r \text{ with } 0 \leq r < y.$$

The numbers q and r are called respectively the *quotient* and *remainder* on division of x by y.

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

$$\text{quot}(x, y) = \text{ the quotient on division of } x \text{ by } y \text{ (where } y \neq 0)$$

is primitive recursive. [6]

(b) Show that the function rem defined by

$$\text{rem}(x, y) = \text{ the remainder on division of } x \text{ by } y \text{ (where } y \neq 0)$$

is primitive recursive. [2]

Question 13

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

$$((-\forall y\ y = x \longrightarrow (-y = x\ \&\ \forall y(y = x \vee \forall y\ y = x))) \longrightarrow (-y = x \vee \forall y\ y = x)) \qquad [3]$$

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

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

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

(b) Write down the tautology used on line (5). $[\frac{1}{2}]$

(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) $\exists x(\phi \rightarrow \psi)$	EI, (6)
(B)	3	(10) $\forall x(\phi \rightarrow \psi)$	UI, (3)

Answer YES or NO. [2]

(iii) The rule UE states that:

> if the formula $\forall v\phi$ occurs on a certain line in a formal proof and
> τ is a term which may be freely substituted for a variable v in ϕ,
> then on any subsequent line we may derive the formula $\phi(\tau/v)$, and
> this formula will depend on the same assumptions as did $\forall v\phi$.

Give a suitable example from everyday mathematics to show that the rule is no longer valid if the underlined passage, which gives a condition on the term τ, is omitted. [3]

Question 14

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

$$\exists z(\forall x\, \forall t\ t = (y + x) \vee \exists y(y \cdot y) = (x + t))$$

(a) $(x \cdot y)$

(b) $(\mathbf{0} + z)$

(c) $(t + x)$

Answer YES or NO in each case. [2]

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

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

(b) $\forall x(\phi \rightarrow \theta),\ \exists x(\psi \vee -\phi) \vdash (\phi \rightarrow -\forall x - (\psi\ \&\ \theta))$, 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) $\forall x(\mathbf{0} \cdot (x + \mathbf{0})) = ((\mathbf{0} \cdot x) + (\mathbf{0} \cdot \mathbf{0}))$

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

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

Question 16

(i) Explain briefly the meaning of *each* of the following statements about a theory T.

(a) T is complete:

(b) T is consistent:

(c) T is axiomatizable. [4]

(ii) Is $\mathbf{0} = \mathbf{1}$ a theorem of the theory Z of elementary Peano arithmetic? Explain your answer briefly. [1]

(iii) Give an example of a theorem of Z which is not a theorem of Q. (No justification is required.) [2]

(iv) Is the theory Z

(a) complete, (b) axiomatizable?

In each case, answer YES or NO. [1]

(v) Which theorem(s) of the course answer(s) the question: *Is arithmetic axiomatizable?*

Explain why the theorem (or theorems) chosen answer(s) the question. (*Your answer may include references to any of the theorems listed in the Logic Handbook.*) [3]

[END OF QUESTION PAPER]