Queen Mary
University of London

B. Sc. Examination by course unit 2011

MTH6128 Number Theory

Duration: 2 hours

Date and time: 8 June 2011, 10:00-12:00

Apart from this page, you are not permitted to read the contents of this question paper until instructed to do so by an invigilator.

You may attempt as many questions as you wish and all questions carry equal marks. Except for the award of a bare pass, only the best 4 questions answered will be counted.

Calculators are NOT permitted in this examination. The unauthorized use of a calculator constitutes an examination offence.

Complete all rough workings in the answer book and cross through any work which is not to be assessed.

Candidates should note that the Examination and Assessment Regulations state that possession of unauthorized materials by any candidate who is under examination conditions is an assessment offence. Please check your pockets now for any notes that you may have forgotten that are in your possession. If you have any, then please raise your hand and give them to an invigilator now.

Exam papers must not be removed from the examination room.

Examiner(s): P. J. Cameron

Question 1 (a) What is meant by the *continued fraction* $[a_0; a_1, \ldots, a_n]$, where $a_0, \ldots, a_n$ are integers and $a_1, \ldots, a_n > 0$? [2]

(b) Find a continued fraction whose value is $\dfrac{78}{101}$. [5]

(c) Find integers x and y satisfying $78x + 101y = 3$. [6]

(d) Find *all* solutions (x, y) to the equation $78x + 101y = 3$ in integers x and y. [7]

(e) Find all solutions (x, y) to the equation $x^2 + y^2 = 65$ in integers x and y. [5]

Question 2 (a) Define *Euler's square bracket function* $[a_0, a_1, \ldots, a_k]$. [3]

(b) Prove by induction that, for $k \geq 0$,

(i) the finite continued fraction $c_k = [a_0; a_1, \ldots, a_k]$ is equal to

$$\frac{[a_0, a_1, \ldots, a_k]}{[a_1, \ldots, a_k]};$$

(ii) the numerator p_k and denominator q_k of this fraction have greatest common divisor 1; and

(iii) $p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}$ if $k \geq 1$.

[13]

(c) Hence show that $|c_k - c_{k-1}| = \dfrac{1}{q_k q_{k-1}}$. [5]

(d) State without proof the inequalities satisfied by the numbers $c_0, c_1, \ldots, c_k$. [4]

Question 3 (a) Define a *quadratic irrational*, and state what it means for a quadratic irrational to be reduced. [5]

(b) Find, with proof, the possible values of the rational number q for which $q + \sqrt{2}$ is a reduced quadratic irrational. [6]

(c) What is meant by the value of an infinite continued fraction $[a_0, a_1, a_2, \ldots]$, where $a_0, a_1, a_2, \ldots$ are integers and $a_1, a_2, \ldots$ are positive? [4]

(d) Which real numbers have a periodic continued fraction? Which have a purely periodic continued fraction? (Proofs not required.) [3]

(e) Find the continued fraction expansion of $\frac{1}{2} + \sqrt{2}$. [7]

Question 4 (a) State a theorem on the representation of prime numbers as the sum of two squares of integers. [2]

(b) Suppose that p is a prime number congruent to 3 (mod 4). Show that p cannot be written as the sum of two squares. Outline how to deduce, from this fact, that the congruence $x^2 \equiv -1 \pmod{p}$ has no solution. [7]

(c) Define the *Legendre symbol* $\left(\dfrac{a}{p}\right)$ where a is an integer and p an odd prime number. [3]

(d) State without proof the values of $\left(\dfrac{-1}{p}\right)$ and $\left(\dfrac{2}{p}\right)$. [4]

(e) Prove that

$$\left(\frac{-2}{p}\right) = \begin{cases} +1 & \text{if } p \equiv 1 \text{ or } 3 \pmod{8}, \\ -1 & \text{if } p \equiv 5 \text{ or } 7 \pmod{8}. \end{cases}$$

[5]

(f) Calculate $\left(\dfrac{45}{61}\right)$. [4]

Question 5 (a) Define a *Pythagorean triple.* [2]

(b) Show that, if the integers (s,t,u) form a Pythagorean triple, then so do $(2st, s^2-t^2, u^2)$. [3]

(c) Hence show that the equation $x^2+y^2=z^{2^n}$ has a solution in positive integers (x,y,z) for all $n \geq 1$. [4]

(d) Find a solution of $x^2+y^2=x^8$ in positive integers. [3]

(e) Describe, with proof, all Pythagorean triples. [13]

Question 6 (a) Let p be a prime number. What is meant by a *primitive root* mod p? [3]

(b) Find a primitive root mod 13, and hence find the orders of all the non-zero elements of $\mathbb{Z}_{13}$. [7]

(c) Does a primitive root mod p exist for every prime number p? Prove your assertion. [10]

(d) Let p be a prime number. Show that there exists an integer w such that $w^3 \equiv 1 \pmod{p}$ and $w \not\equiv 1 \pmod{p}$, if and only if $p \equiv 1 \pmod{3}$. Find such an integer w in the case $p = 13$. [5]

Question 7 (a) What is a (binary) *quadratic form* in variables x,y over the integers? [3]

(b) Define the terms *positive definite*, *negative definite*, and *indefinite* for quadratic forms. Give tests for recognising whether these properties hold, in terms of the coefficients of the form. Must every quadratic form have one of these properties? [5]

(c) In each of the following cases, state whether the quadratic form is positive definite, negative definite, indefinite, or none of these:

$$\text{(i) } 2x^2+3xy+y^2, \qquad \text{(ii) } 2x^2-12xy+18y^2, \qquad \text{(iii) } x^2-2xy+2y^2.$$

[6]

(d) What is meant by saying that a positive definite quadratic form is *reduced*? What is meant by saying that two quadratic forms are *equivalent*? [4]

(e) State a theorem about the equivalence of positive definite forms to reduced forms. [3]

(f) Find a reduced form equivalent to $x^2+2xy+2y^2$. [4]

End of Paper