Queen Mary
University of London

B. Sc. Examination by course unit 2010

MTH6128 Number Theory

Duration: 2 hours

Date and time: 14 May 2010, 14:30–16:30

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) State the Chinese Remainder Theorem. [4]

(b) Find the general solution of the simultaneous congruences

$$x \equiv 3 \pmod 7, \qquad x \equiv 1 \pmod{11}.$$ [4]

(c) State and prove Fermat's Little Theorem. [9]

(d) Use Fermat's Little Theorem to prove that, for any integer n,

$$n^{37} \equiv n \pmod{13} \quad \text{and} \quad n^{37} \equiv n \pmod{19}.$$ [4]

(e) Deduce that, for any integer n,

$$n^{37} \equiv n \pmod{741}.$$ [4]

Question 2 (a) Use Euclid's Algorithm to find $\gcd(321, 210)$. [4]

(b) Find integers x, y satisfying $321x + 210y = d$, where $d = \gcd(321, 210)$. [4]

(c) Does the equation $321x + 210y = 17$ have a solution in integers x, y? If so, find one; if not, explain why not. [4]

(d) State, without proof, a necessary and sufficient condition, in terms of the integers a, b, c, for the equation $ax + by = c$ to have a solution in integers x, y. [5]

(e) What is a finite continued fraction? [4]

(f) Find a continued fraction for $\dfrac{321}{210}$. [4]

Question 3 (a) Let $a_0, a_1, \ldots$ be positive integers. Explain carefully what is meant by the value of the infinite continued fraction $[a_0; a_1, a_2, \ldots]$. State which numbers can be the value of such a continued fraction. [5]

(b) State which numbers can be the value of a periodic continued fraction

$$[a_0; a_1, \ldots, a_{l-1}, \overline{a_l, \ldots, a_{l+k-1}}],$$

explaining the notation. [4]

(c) Find the value of the continued fraction $[\overline{1; 8}]$, explaining your calculations. [8]

(d) Find a continued fraction whose value is $2\sqrt{2} - 1$, explaining your calculations. [8]

Question 4 You are given that

$$\sqrt{31} = [5; \overline{1, 1, 3, 5, 3, 1, 1, 10}].$$

For each of the following equations, say whether it has a solution in positive integers x, y or not. If there is a solution, you should find one; if not, you should explain why not.

(a) $31 = x^2 + y^2$; [7]

(b) $x^2 - 31y^2 = -1$; [9]

(c) $x^2 - 31y^2 = 1$. [9]

You should state carefully any theorems you use about the solutions to equations of these types.

Question 5 (a) What is a *primitive root* in $\mathbb{Z}_p$ (the integers mod p), where p is prime? [3]

(b) How many primitive roots are there in $\mathbb{Z}_{181}$? [5]

(c) Show that 2 is a primitive root in $\mathbb{Z}_{19}$. [5]

(d) Find the orders of all the elements of $\mathbb{Z}_{19}$, explaining your method. [6]

(e) Show that a non-zero element of $\mathbb{Z}_p$ is a quadratic residue if and only if it is an even power of a primitive root. Hence find the quadratic residues in $\mathbb{Z}_{19}$. [6]

Question 6 (a) Define the *Legendre symbol* $\left(\frac{a}{p}\right)$, where a is an integer and p is an odd prime. [3]

(b) Prove that

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p},$$

and deduce that $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. [4]

(c) State the values of $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$. [4]

(d) State the Law of Quadratic Reciprocity. [4]

(e) Calculate the value of $\left(\frac{43}{71}\right)$. [5]

(f) Prove that, if p is a prime greater than 3, then

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

Question 7 (a) What does it mean to say that the quadratic form $Q(x,y) = ax^2 + bxy + cy^2$ is (i) positive definite, (ii) negative definite, (iii) indefinite? [6]

(b) True or false? *Every quadratic form is of one of the above types.* Give reasons for your answer. [3]

(c) For each of the following quadratic forms, determine if it is positive definite, negative definite, or indefinite:

(i) $x^2 - 2xy$, (ii) $x^2 + xy + y^2$, (iii) $x^2 - 2xy + y^2$. [6]

(d) What does it mean to say that two quadratic forms are *equivalent*? [3]

(e) What does it mean to say that a positive definite quadratic form is *reduced*? How many reduced quadratic forms are equivalent to a given positive definite form? [3]

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

End of Paper