Queen Mary
University of London

B. Sc. Examination by course unit 2012

MTH6128 Number Theory

Duration: 2 hours

Date and time: 8 June 2012, 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) Use the Euclidean algorithm to find the greatest common divisor of 263 and 108. [4]

(b) Use your working to find x and y satisfying $263x+108y=1$. [4]

(c) Use your working to find a continued fraction expansion of $\frac{263}{108}$. [4]

(d) Write down a different continued fraction expansion of $\frac{263}{108}$, explaining what this means. [3]

(e) Suppose that x' and y' are any integers satisfying $263x'+108y'=1$. Show that $263(x'-x)=108(y-y')$, where x and y are the numbers you cound in part (b). Hence show that $x'=x+108t$, $y'=y-263t$ for some integer t. [6]

(f) Hence find x' and y', different from the x and y you found in part (b), satisfying $263x'+108y'=1$. [4]

Question 2 (a) Define Euler's *square bracket function*, and explain its connection with continued fractions. [5]

(b) Which real numbers have

(i) finite continued fractions;

(ii) periodic continued fractions;

(iii) purely periodic continued fractions?

(Proofs not required.) [6]

(c) Explain how to use the continued fraction for $\sqrt{n}$ (where n is a positive integer which is not a square) to find the solutions of the equations $x^2-ny^2=\pm1$ in positive integers (x,y). [5]

(d) Given that

$$\sqrt{29}=[5;\overline{2,1,1,2,10}],$$

find the smallest solution of $x^2-29y^2=1$ in positive integers. [9]

Question 3 (a) State the *Chinese Remainder Theorem*. [3]

(b) Define *Euler's totient function* $\phi(n)$. [2]

(c) Use the Chinese Remainder Theorem to show that, if $\gcd(m,n)=1$, then $\phi(mn)=\phi(m)\phi(n)$. [5]

(d) If p is prime and $a\geq1$, what is the value of $\phi(p^a)$? Prove your assertion. [6]

(e) Prove that, if $\gcd(a,n)=1$, then $a^{\phi(n)}\equiv1 \pmod{n}$. [6]

(f) Show that $a^2\equiv1 \pmod{8}$ for any odd number a. [3]

Question 4 In this question, p denotes an odd prime.

(a) Define a *quadratic residue* mod p. [3]

(b) Define the *Legendre symbol* $\left(\dfrac{a}{p}\right)$ for any integer a. [4]

(c) State the *Law of Quadratic Reciprocity*. [3]

(d) Calculate the following Legendre symbols:

$$\text{(i)}\ \left(\frac{60}{43}\right), \qquad \text{(ii)}\ \left(\frac{-3}{43}\right).$$

You should state clearly any rules for computing Legendre symbols that you use, but are not required to prove them. [6]

(e) Suppose that $p = x^2 + y^2$ for some integers x and y. Show that

$$\left(\frac{x^2}{p}\right) = \left(\frac{-y^2}{p}\right),$$

and deduce that $\left(\dfrac{-1}{p}\right) = 1$. [5]

(f) Is it true that any odd prime p satisfying $\left(\dfrac{-1}{p}\right) = 1$ is a sum of two squares of integers? (Give brief reasons; detailed proof not required.) [4]

Question 5 (a) What is a *quadratic form* in variables x, y over the integers? [2]

(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. [6]

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

$$\text{(i)}\ x^2 + 4xy + 5y^2, \qquad \text{(ii)}\ 9x^2 - 24xy + 16y^2.$$

[4]

(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) Show that the quadratic forms $x^2 + y^2$ and $x^2 + 4xy + 5y^2$ are equivalent. [3]

(f) Hence give a description, in terms of their prime factors, of the integers represented by the quadratic form $x^2 + 4xy + 5y^2$. Explain briefly why your description is correct; a detailed proof is not required. [6]

Question 6 (a) Prove that any prime greater than 3 is congruent to 1 or 5 (mod 6). [2]

(b) Prove that there are infinitely many prime numbers congruent to 5 (mod 6). [5]

(c) Show that $\left(\frac{-3}{p}\right) = +1$ if and only if $p \equiv 1 \pmod{6}$. [**Hint:** You may want to consider the possible congruence class of p (mod 12).] [8]

(d) Let $q_1, \ldots, q_n$ be prime numbers congruent to 1 (mod 6). Use the result of the preceding part to show that any prime divisor of $(2q_1 \cdots q_n)^2 + 3$ is congruent to 1 (mod 6). [7]

(e) Hence show that there are infinitely many prime numbers congruent to 1 (mod 6). [3]

End of Paper