Queen Mary
University of London

B. Sc. Examination by course unit 2013

MTH6128 Number Theory

Duration: 2 hours

Date and time: 29 May 2013, 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.

Important note: the Academic Regulations state that possession of unauthorized material at any time by a student who is under examination conditions is an assessment offence and can lead to expulsion from QMUL.

Please check now to ensure you do not have any notes, mobile phones or unauthorised electronic devices on your person. If you have any, then please raise your hand and give them to an invigilator immediately. Please be aware that if you are found to have hidden unauthorised material elsewhere, including toilets and cloakrooms, it will be treated as being found in your possession. Unauthorised material found on your mobile phone or other electronic device will be considered the same as being in possession of paper notes. Disruption caused by mobile phones is also an examination offence.

Exam papers must not be removed from the examination room.

Examiner(s): I. Tomašić

Question 1 (a) Using the Euclidean algorithm or otherwise, find the continued fraction expansion of $\dfrac{127}{24}$. [5]

(b) Find the value of the periodic continued fraction $[\overline{10;3,2,3}]$. [8]

(c) Find the value of the periodic continued fraction $[5;\overline{3,2,3,10}]$. [2]

(d) 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 $x^2 - ny^2 = \pm 1$ in positive integers (x, y). [4]

(e) Using your answers to parts (c) and (d), find the fundamental solution to the equation [4]

$$x^2 - 28y^2 = \pm 1.$$

(f) Does the equation $x^2 - 28y^2 = -1$ have a solution in integers x, y? Explain! [2]

Question 2 (a) Find the continued fraction for $\sqrt{53}$. [10]

(b) Explain how to use the continued fraction for $\sqrt{p}$ (where p is a prime congruent to 1 modulo 4) to find the solutions of the equations $x^2 + y^2 = p$ in positive integers (x, y). [5]

(c) Using parts (a) and (b), find positive integers x and y such that $x^2 + y^2 = 53$. [5]

(d) Prove the following statement. If n is an integer congruent to 3 modulo 4, then the equation $x^2 + y^2 = n$ does not have a solution in integers x, y. [5]

Question 3 (a) What is an *algebraic number*? What is a *transcendental number*? [3]

(b) What is an *algebraic integer*? [2]

(c) Which of the following numbers are algebraic integers? Explain, stating precisely all theorems you use!

(i) $\sqrt{3} + \sqrt[3]{2}$;

(ii) $\dfrac{3 + \sqrt{7}}{2}$; [8]

(iii) $\dfrac{5 + 3\sqrt{17}}{2}$;

(iv) $\dfrac{5 + 7\sqrt{13}}{3}$.

(d) What do we mean by saying that an irrational number x is *approximable by rationals to order m*? [3]

(e) Prove that every positive irrational is approximable by rationals to order 2. [4]

(f) Let

$$x = \sum_{i=1}^{\infty} \frac{1}{2^{i!}} = \frac{1}{2^{1!}} + \frac{1}{2^{2!}} + \frac{1}{2^{3!}} + \cdots.$$

Is x algebraic? Prove your claim! [5]

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

(a) Define a *quadratic residue* mod p. [2]

(b) Define the *Legendre symbol* $\left(\frac{a}{p}\right)$ for any integer a. [3]

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

(d) Calculate the value of $\left(\frac{21}{53}\right)$. [6]

(e) Suppose that p can be represented as $p = x^2 - 3y^2$.

(i) Show that $\left(\frac{x^2}{p}\right) = \left(\frac{3y^2}{p}\right)$. [2]

(ii) Deduce, using quadratic reciprocity, that for such primes p we have [4]

$$\left(\frac{p}{3}\right) = (-1)^{(p-1)/2}.$$

(iii) Considering the cases $p \equiv \pm 1 \pmod 4$, deduce that p must be congruent to 1 or 11 modulo 12. [5]

Question 5 (a) What is the *discriminant* of the quadratic form $f(x,y) = ax^2 + bxy + cy^2$ over the integers? [1]

(b) Define the following terms for binary quadratic forms:

(i) *positive definite*;

(ii) *negative definite*;

(iii) *indefinite*;

(iv) *degenerate*.

For each case, give a test for recognising whether these properties hold, in terms of the coefficients of the form. [8]

(c) In each of the following cases, state whether the quadratic form is positive definite, negative definite, indefinite, or degenerate:

(i) $-3x^2 + 7xy + 2y^2$,

(ii) $x^2 - 2xy + 6y^2$, [3]

(iii) $x^2 - 2xy + 1$.

(d) What is meant by saying that a positive definite binary quadratic form is *reduced*? [2]

(e) What is meant by saying that two binary quadratic forms are *equivalent*? When are two reduced quadratic forms equivalent? [4]

(f) Show that the quadratic forms $6x^2 - 2xy + y^2$ and $7x^2 - 22xy + 18y^2$ are *not* equivalent. [7]

Question 6 (a) Prove that there are infinitely many prime numbers congruent to 3 (mod 4). [5]

(b) Use part (a) to deduce that there exist infinitely many primes which are *not* congruent to 1 modulo 8. [2]

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

(d) Let x be an even integer. Show that every prime divisor p of x^4+1 satisfies

$$\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = 1$$

and that this implies $p \equiv 1 \pmod 8$. [**Hint:** Observe that $x^4+1 = (x^2+1)^2 - 2x^2$.] [8]

(e) Let $q_1, \ldots, q_n$ be prime numbers congruent to 1 (mod 8). By the preceding part it follows that that any prime divisor of $(2q_1 \cdots q_n)^4 + 1$ is congruent to 1 (mod 8). Using this fact, show that there are infinitely many prime numbers congruent to 1 (mod 8). [6]

End of Paper