Queen Mary
University of London

MTH6128 / MTH6128P: Number Theory

Duration: 2 hours

Date and time: 2 June 2016, 10:00 to 12:00

You should attempt ALL questions. Marks awarded are shown next to the questions.

Calculators are **not** permitted in this examination. The unauthorised use of a calculator constitutes an examination offence.

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

Possession of unauthorised material at any time when under examination conditions is an assessment offence and can lead to expulsion from QMUL. Check now to ensure you do not have any notes, mobile phones, smartwatches or unauthorised electronic devices on your person. If you do, raise your hand and give them to an invigilator immediately. It is also an offence to have any writing of any kind on your person, including on your body. If you are found to have hidden unauthorised material elsewhere, including toilets and cloakrooms it shall 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. A mobile phone that causes a disruption in the exam is also an assessment offence.

Exam papers must not be removed from the examination room.

Examiner(s): X. Li

 Turn Over

Question 1.

(a) Define the terms

(i) **algebraic number**;

(ii) **algebraic integer**; [**4**]

(iii) **transcendental number**.

(b) Which of the following numbers are algebraic integers? Explain, stating explicitly which theorems you use.

(i) $\dfrac{5+\sqrt{15}}{2}$; [**5**]

(ii) $\dfrac{1}{2}\sqrt{41}-\dfrac{3}{2}$.

(c) What does it mean for a positive irrational number to be *approximable by rationals to order m*? [**3**]

(d) Is $\sqrt[3]{2}$ approximable by rationals to order 4? Justify your answer. State explicitly which theorems you use in the proof. [**6**]

Question 2.

(a) Find the continued fraction for $\dfrac{7+\sqrt{11}}{3}$. [**8**]

(b) Calculate the value of the infinite continued fraction $[2;\overline{4,1}]$. [**8**]

Question 3.

(a) You are given that

$$[8;\overline{1,1,5,5,1,1,16}]$$

is the continued fraction for $\sqrt{73}$. Using this, find positive integers x and y such that $x^2+y^2=73$. [**6**]

(b) You are given that

$$[8;\overline{1,1,1,16}]$$

is the continued fraction for $\sqrt{75}$. Using this, find all the integer solutions of the equation

$$x^2-75y^2=\pm 1.$$

Explain why you have found ALL the integer solutions. [**8**]

(c) Let n be a positive integer which is not a square. Suppose that x, y and x', y' are positive integers satisfying $x^2-ny^2=\pm 1$ and $(x')^2-n(y')^2=\pm 1$. Assume that $x<x'$.

Show that $y<y'$. State explicitly which theorems you use in the proof. [**8**]

Question 4.

(a) Let p be a prime. What is a **primitive root** (mod p)? [**3**]

(b) Find a primitive root (mod 11). [**5**]

(c) Find an integer n with $n^5 \equiv 1 \pmod{11}$ and $n^4 \not\equiv 1 \pmod{11}$. Show that the integer you have found has the required properties. [**3**]

(d) Does there exist an integer n with $n^3 \equiv 1 \pmod{11}$ and $n^2 \not\equiv 1 \pmod{11}$? Justify your answer. State explicitly which theorems you use in the proof. [**5**]

Question 5.

(a) Let p be an odd prime. What is a **quadratic residue** (mod p)? [**2**]

(b) Let p be an odd prime, and let a be an integer. Define the **Legendre symbol** $\left(\frac{a}{p}\right)$. [**3**]

(c) Calculate the value of $\left(\frac{18}{71}\right)$. You should state clearly any rules for computing Legendre symbols that you use, but are not required to prove them. [**6**]

(d) Let p be an odd prime. Show that we have [**5**]

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} +1 & \text{if } p \equiv 1 \pmod{4}, \\ -1 & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

Question 6.

(a) What is a **quadratic form** over the integers? [**2**]

(b) Give an example of a quadratic form which is indefinite. Explain why the example you gave has the desired property. [**2**]

(c) Find a reduced positive definite quadratic form which is equivalent to [**4**]

$$3x^2 + 2xy + y^2.$$

(d) What is meant by saying that an integer is *represented* by a quadratic form? What can we say about the integers represented by two equivalent quadratic forms? [**4**]

End of Paper.