Queen Mary
University of London

Main Examination period 2019

MTH6128 / MTH6128P: Number Theory

Duration: 2 hours

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 should attempt ALL questions. Marks available 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 work 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 unauthorised 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 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. 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.

Examiners: S. Lester, A. Saha

Question 1. [20 marks]

(a) Define the terms **algebraic number** and **minimal polynomial**. State the **Chinese Remainder Theorem**. **[6]**

(b) Give an example of an algebraic integer, which is not an integer. Explain why the number you gave has the desired properties. **[3]**

(c) Find all integer solutions to the system of congruences

$$\begin{aligned} x &\equiv 1 \pmod{7} \\ x &\equiv 2 \pmod{30}. \end{aligned}$$

Explain your working. **[6]**

(d) Determine the minimal polynomial of $\dfrac{\sqrt{7}}{2} - \dfrac{9}{2}$. **[5]**

Question 2. [15 marks]

(a) Find the value of the continued fraction

$$[4; \overline{1, 6}].$$

Your answer should be a number of the form $u + v\sqrt{d}$, where $u, v \in \mathbb{Q}$, $d \in \mathbb{N}$. **[5]**

(b) Let x be an irrational number and n be a positive integer. Let $c_n = p_n/q_n$ be the nth convergent of the continued fraction of x.

(i) Prove that **[5]**

$$\frac{1}{q_n q_{n+1}} = \left| \frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n} \right| = \left| x - \frac{p_{n+1}}{q_{n+1}} \right| + \left| x - \frac{p_n}{q_n} \right|.$$

State precisely all results from the lectures you use in the proof.

(ii) Prove that $\dfrac{1}{q_n q_{n+1}} < \dfrac{1}{2q_n^2} + \dfrac{1}{2q_{n+1}^2}$. **[2]**

(iii) Use parts (i) and (ii) to prove that **[3]**

$$\left| x - \frac{p_n}{q_n} \right| < \frac{1}{2q_n^2} \qquad \text{or} \qquad \left| x - \frac{p_{n+1}}{q_{n+1}} \right| < \frac{1}{2q_{n+1}^2}.$$

Question 3. [15 marks]

(a) Given that

$$\sqrt{19} = [4; \overline{2, 1, 3, 1, 2, 8}],$$

find the fundamental solution to

$$x^2 - 19y^2 = \pm 1.$$

Use your answer to write down all positive integer solutions to the equation $x^2 - 19y^2 = 1$. Explain why you have found ALL solutions. **[9]**

(b) Given that $25^2 \equiv -1 \pmod{313}$ use Hermite's algorithm to find integers x, y such that

$$x^2 + y^2 = 313.$$ **[6]**

Question 4. [13 marks]

(a) Define **Euler's ϕ-function**. Define the term **primitive root** $\pmod{p}$, where p is prime. **[4]**

(b) Find a primitive root $\pmod{29}$. Explain why the integer you gave has the desired properties. **[5]**

(c) Find the number of primitive roots $\pmod{101}$. Explain your working. **[4]**

Question 5. [25 marks]

(a) Define the term **quadratic residue**. State **Euler's Criterion.** **[5]**

(b) For each of the equations, find all integers strictly between 0 and 53 which are solutions to the following equations. Use the methods developed in the lectures to solve the equation $x^2 \equiv a \pmod{p}$ and explain your working.

(i) $x^2 \equiv 35 \pmod{53}$ **[6]**

(ii) $x^2 \equiv -1 \pmod{53}$ **[6]**

(c) Prove there are infinitely many prime numbers congruent to $1 \pmod{4}$. **[8]**

Question 6. [12 marks]

(a) State **Hensel's Lemma**. **[3]**

(b) Use Hensel's Lemma to find all integer solutions to the equation

$$x^2 - 5 \equiv 0 \pmod{19^2}.$$

Explain your working. **[9]**

End of Paper.