Queen Mary
University of London

Main Examination period 2020 – May – Semester B

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, S. Sasaki

Question 1 [20 marks].

(a) Define the terms **algebraic integer** and **quadratic integer**. State the Fundamental Theorem of Arithmetic. **[6]**

(b) Determine which of the following numbers are quadratic integers. Explicitly state any results from the lectures that you use. **[4]**

(i) $\dfrac{2+\sqrt{52}}{4}$;

(ii) $\dfrac{\sqrt{43}}{2}-\dfrac{7}{2}$.

(c) Show that $\sqrt{3+\sqrt{11}}$ is an algebraic integer. **[5]**

(d) Find all integer solutions to the equation **[5]**

$$17x \equiv 4 \pmod{71}.$$

Question 2 [11 marks].

(a) Use the Euclidean algorithm to find a continued fraction expansion of $\dfrac{1723}{505}$. **[4]**

(b) Let $a_0, a_1, \ldots, a_n$ be positive integers. Let $c_k = p_k/q_k$ be the kth convergent of the continued fraction $[a_0; a_1, \ldots, a_n]$.

(i) Prove for each $1 \leqslant k \leqslant n$ that **[2]**

$$\frac{p_k}{p_{k-1}} = a_k + \frac{p_{k-1}}{p_{k-2}}.$$

(ii) Use part (i) to prove that for each $1 \leqslant k \leqslant n$ **[5]**

$$\frac{p_k}{p_{k-1}} = [a_k; a_{k-1}, \ldots, a_1, a_0].$$

Question 3 [15 marks].

(a) Find the continued fraction expansion of $\dfrac{1+\sqrt{37}}{2}$. **[6]**

(b) You are given that

$$\sqrt{53} = [7; \overline{3, 1, 1, 3, 14}].$$

Find all solutions in positive integers x, y to the following equation

$$x^2 - 53y^2 = -1.$$

Explain why you have found ALL solutions. **[9]**

Question 4 [19 marks].

(a) Given a positive integer n define the **order of** $x \pmod{n}$. State Euler's Theorem. **[4]**

(b) Find the last two digits of 3^{40845}. Explain your working. **[5]**

(c) Let m and n be positive integers. Prove that $\phi(mn) \leqslant \phi(m)\phi(n)$. **[5]**

(d) Find a primitive root $\pmod{17}$. Explain why the integer you gave has the desired properties. **[5]**

Question 5 [20 marks].

(a) Define the term **quadratic non-residue**. Define the **Legendre symbol** $\left(\dfrac{a}{p}\right)$. State the Law of Quadratic Reciprocity. **[6]**

(b) Calculate the value of $\left(\dfrac{99}{101}\right)$. You should clearly state any rules you use for calculating the Legendre symbol. **[6]**

(c) State and prove Euler's Criterion. **[8]**

Question 6 [15 marks].

(a) For each of the equations, determine whether there exists a solution x, y in positive integers. If a solution exists explain why. If no solution exists explain why not. Explicitly state any results from the lectures that you use. **[6]**

(i) $x^2 + y^2 = 5850$;

(ii) $x^2 + y^2 = 9450$.

(b) Use Hensel's Lemma to find all integer solutions to the equation **[9]**

$$x^2 \equiv 3 \pmod{11^2}.$$

Explain your working.

End of Paper.