Queen Mary
University of London

**Main Examination period 2018**

# 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 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.**

**Examiners: S. Lester, X. Li**

**Question 1. [20 marks]**

(a) Define the terms **algebraic integer**, **quadratic integer**, and **transcendental number**. **[6]**

(b) Determine which of the following are quadratic integers. Explain which theorems you have used. **[8]**

(i) $\frac{1+\sqrt{49}}{2}$;

(ii) $\frac{\sqrt{3}}{2} - \frac{7}{2}$;

(iii) $\frac{\sqrt{5}}{2} + \frac{\sqrt{-3}}{2}$;

(iv) $\frac{7}{2} + \frac{\sqrt{65}}{2}$.

(c) Let $D$ be a natural number which is not a square. Using minimal polynomials, show that $\frac{1+\sqrt{D}}{2}$ is an algebraic integer if and only if $D \equiv 1 \pmod 4$. **[6]**

**Question 2. [20 marks]**

(a) What is a **periodic continued fraction**? Give an example of an irrational number whose continued fraction expansion is not periodic. You do not need to justify your answer. **[4]**

(b) Use the Euclidean algorithm to find a continued fraction expansion for $\dfrac{241}{113}$. **[5]**

(c) Determine the value of the infinite continued fraction

$$[1; \overline{2, 1}].$$

Write your answer in the form $u + v\sqrt{d}$, where $u, v \in \mathbb{Q}$ and $d \in \mathbb{Z}$. **[5]**

(d) Find the continued fraction expansion of $\sqrt{7}$. **[6]**

**Question 3. [20 marks]**

(a) Given that

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

find the fundamental solution to the equation

$$x^2 - 29y^2 = \pm 1.$$

Use your answer to write down all positive integer solutions to the equation $x^2 - 29y^2 = \pm 1$. Explain why you have found ALL solutions. **[8]**

(b) Given that $37^2 \equiv -1 \pmod{137}$ use Hermite's algorithm to find integers $x, y$ such that

$$x^2 + y^2 = 137.$$

**[8]**

(c) Suppose that $n \equiv 3 \pmod 4$. Show that $x^2 + y^2 = n$ has no integer solutions. **[4]**

**Question 4. [20 marks]**

(a) Given a positive integer $n$ and an integer $x$ such that $\gcd(x, n) = 1$, define the **order of** $x \pmod{n}$. Define the term **primitive root** $\pmod{p}$, where $p$ is prime. **[4]**

(b) Find a primitive root (mod 13). How many primitive roots (mod 13) are there? **[4]**

(c) Does there exist an integer $n$ such that $n^4 \not\equiv 1 \pmod{17}$ and $n^5 \equiv 1 \pmod{17}$? Justify your answer by stating explicitly which theorems you use in the proof. **[6]**

(d) Compute $\varphi(280)$. (Hint: $280 = 2^3 \cdot 5 \cdot 7$.) **[3]**

(e) Show that $\varphi(n)$ is even for $n > 2$. **[3]**

**Question 5. [20 marks]**

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

(b) Both 227 and 137 are primes. Compute $\left(\frac{137}{227}\right)$. You should clearly state any rules you use for calculating the Legendre symbol. **[7]**

(c) Let $p$ be an odd prime. Suppose that $p + 2$ is also prime. Show that $p$ is a quadratic residue $\pmod{(p+2)}$ if and only if

$$p \equiv \pm 1 \pmod{8}.$$ **[7]**

---

**End of Paper.**