Queen Mary
University of London

Main Examination period 2021 – January – Semester A

MTH5130: Number Theory

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

In completing this assessment, you may use books, notes, and the Internet. You may use calculators and computers, but you must show your work for any calculations you do. You must not seek or obtain help from anyone else.

At the start of your work, please **copy out and sign** the following declaration:

> I declare that my submission is entirely my own, and I have not sought or obtained help from anyone else.

All work should be **handwritten** and should **include your student number**.

The exam is available for a period of **24 hours**. Upon accessing the exam, you will have **3 hours** in which to complete and submit this assessment.

When you have finished your work:

- scan your work, convert it to a **single PDF file**, and submit this file on QMPlus;
- e-mail a copy to **maths@qmul.ac.uk** with your student number and the module code in the subject line;
- with your e-mail, include a photograph of the first page of your work together with either yourself or your student ID card.

You are expected to spend about **2 hours** to complete the assessment, plus the time taken to scan and upload your work. Please try to upload your work well before the end of the submission window, in case you experience computer problems. **Only one attempt is allowed – once you have submitted your work, it is final**.

Examiners: S. Sasaki, J. Bray

Continue to next page

Question 1 [17 marks].

(a) State Fermat's Little Theorem, and use it to prove that 15 is a composite number. **[6]**

(b) Let ϕ be Euler's totient function. What is the parity of $\phi(15841)$? Justify your answer. State clearly any results you use from the lecture material without proofs. **[3]**

(c) Find all the primitive roots mod 11 in $\{1, 2, \ldots, 10\}$. Justify your answer. **[8]**

Question 2 [10 marks]. Using the Chinese Remainder Theorem, solve the following simultaneous congruence equations in x. Show all your working.

$$\begin{aligned} 9x &\equiv 3 \mod 15, \\ 5x &\equiv 7 \mod 21, \\ 7x &\equiv 4 \mod 13. \end{aligned}$$ **[10]**

Question 3 [30 marks].

(a) Assume that 3083 and 3911 are prime numbers. Using properties of Legendre symbols, compute the Legendre symbol $\left(\frac{3083}{3911}\right)$. Justify your answer. **[8]**

(b) Which of the following congruences are soluble? If soluble, find a positive integer solution less than 79; if insoluble, explain why.

(i) $x^2 \equiv 41 \mod 79$. **[4]**

(ii) $41x^2 \equiv 43 \mod 79$. **[8]**

(c) Using Hensel's Lemma, find an integer $1 \leq z \leq 125$ satisfying $z^3 \equiv 2 \mod 125$. Show all your working. **[10]**

 Continue to next page

Question 4 [20 marks].

(a) Compute the continued fraction expression of $\sqrt{11}$. **[4]**

(b) Compute the convergents $\frac{s_0}{t_0}, \frac{s_1}{t_1}, \frac{s_2}{t_2}$ and $\frac{s_3}{t_3}$ to $\sqrt{11}$. **[4]**

(c) Find the smallest and the fourth smallest positive integer solutions to the equation

$$x^2 - 11y^2 = \pm 1.$$ **[6]**

(d) Compute the convergent $\frac{s_7}{t_7}$. **[6]**

Question 5 [10 marks]. Use $67^2 \equiv -1 \bmod 449$ and Hermites' algorithm to find a pair of positive integers s and t such that

$$s^2 + t^2 = 449.$$ **[10]**

Question 6 [13 marks].

(a) What is the definition of a unit in a ring R? **[3]**

(b) How many units are there in the following rings? If finitely many, list them all; if infinitely many, describe them all.

(i) $\mathbb{Z}[\sqrt{-1}]$. **[4]**

(ii) $\mathbb{Z}[\sqrt{11}]$. **[6]**

End of Paper.