Main Examination period 2022 – 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 and notes.**
- **You may use calculators and computers, but you must show your working for any calculations you do.**
- **You may use the Internet as a resource, but not to ask for the solution to an exam question or to copy any solution you find.**
- **You must not seek or obtain 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:

- scan your work, convert it to a **single PDF file**, and submit this file using the tool below the link to the exam;
- 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.

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, B. Noohi

Question 1 [18 marks].

(a) Find an integer $1 \leq z \leq 143$ satisfying $z \equiv 3^{143} \bmod 143$. Show your working. (Hint: $143 = 2^7 + 2^3 + 2^2 + 2^1 + 1$ and $3^{16} \equiv 3 \bmod 143$.) [**6**]

(b) Use (a) to show that 143 is not a prime number. State clearly any result you are using from lectures. [**3**]

(c) Let p be a prime number and let z be a primitive root mod p. Prove that

$$1, z, z^2, \ldots, z^{p-2}$$

are all distinct mod p. [**9**]

Question 2 [15 marks]. Let $p > 3$ be a prime number. State clearly any results you are using from lectures and prove the following:

(a)

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

[**3**]

(b)

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

[**3**]

(c)

$$\left(\frac{3}{p}\right) = \begin{cases} +1 & \text{if } p \equiv 1 \text{ or } 11 \bmod 12, \\ -1 & \text{if } p \equiv 5 \text{ or } 7 \bmod 12. \end{cases}$$

[**9**]

Question 3 [21 marks].

(a) Which of the following congruences are soluble? If soluble, find a positive integer solution less than 47; if insoluble, explain why.

(i) $x^2 \equiv 41 \bmod 47$. [**4**]

(ii) $3x^2 \equiv 32 \bmod 47$. [**8**]

(b) Using Hensel's lemma, find all integers $1 \leq z \leq 125$ satisfying $z^2 + z \equiv -3 \bmod 125$. [**9**]

Question 4 [18 marks].

(a) Compute the continued fraction expression for $\sqrt{23}$. Show your working. [**4**]

(b) Compute the convergents $\frac{s_1}{t_1}, \frac{s_2}{t_2}, \frac{s_3}{t_3}$ to $\sqrt{23}$. Show your working. [**4**]

(c) By working out the second smallest positive solution to the equation $x^2 - 23y^2 = 1$, compute the convergent $\frac{s_7}{t_7}$. [**10**]

Question 5 [18 marks].

(a) Using that 137 is a prime number, find all solutions to

$$x^2 \equiv -1 \mod 137$$

satisfying $1 \leq x \leq 137$. Show your working. [**9**]

(b) Using (a), write 137 as a sum of two squares. Show your working. State clearly any results you are using from lectures. [**9**]

Question 6 [10 marks]. What are the units of $\mathbb{Z}[\sqrt{15}]$? Describe them all. Justify your answer. [**10**]

End of Paper.