The University Of Sheffield.

SCHOOL OF MATHEMATICS AND STATISTICS **Autumn 2020**

Topics in Number Theory

This is an open book exam. Answer all questions. You can work on the exam during the 24 hour period starting at 10am (GMT), and you must submit your work within 3 hours of accessing the exam paper or by the end of the 24 hour period (whichever is earlier). ***Late submission will not be considered without extenuating circumstances.*** *Unless it is explicitly stated otherwise, it is intended that calculations are performed by hand (possibly with the aid of a calculator). To gain full marks, you will need to show your working. By uploading your solutions you declare that your submission consists entirely of your own work, that any use of sources or tools other than material provided for this module is cited and acknowledged, and that no unfair means have been used.*

You can rely on the materials in MAS330 MOLE/Blackboard page, including problem sheets and solutions. However you need to show the methods that you are using: answers without justification will not be accepted. There are four questions, each worth 15 marks. Parts (i), (ii), (iii) in each question are typically not related to each other. However, please try to follow the order of the questions in the paper you upload.

1 (i) (a) Give an example of $\overline{a}, \overline{b} \in \mathbb{Z}_{143}$ such that $\overline{a} \neq 0$, $\overline{b} \neq 0$ but $\overline{a} \cdot \overline{b} = 0$. ***(2 marks)***

(b) Prove that if $\overline{a}, \overline{b} \in \mathbb{Z}_{43}$, then

$$\overline{a} \cdot \overline{b} = 0 \implies \overline{a} = 0 \text{ or } \overline{b} = 0.$$

(2 marks)

(ii) Explain why $\overline{19}$ is invertible in $\mathbb{Z}_{143}^{\star}$ and find its inverse. ***(5 marks)***

(iii) Compute $2021^{2020} \pmod{143}$. ***(6 marks)***

2 (i) Find all primitive roots in $\mathbb{Z}_{19}^{\star}$. ***(6 marks)***

(ii) Find all solutions of $\phi(n) = 18$. ***(6 marks)***

(iii) Let p be a prime and let $G = \mathbb{Z}_p \times \mathbb{Z}_p$ be the group consisting of pairs $(\overline{a}, \overline{b})$ and component-wise addition. Prove that G is not cyclic. ***(3 marks)***

3 (i) Compute the Legendre symbol $\left(\dfrac{266}{383}\right)$. ***(5 marks)***

(ii) Use quadratic reciprocity to explain how many solutions there are for $x^3 - 1 = 0$ in $x \in \mathbb{Z}_p$, explicitly for all p (you do not need to find the solutions). ***(5 marks)***

(iii) (a) Let q be an odd prime. Show that

$$2^{2^n} \equiv -1 \pmod{q} \implies 2^{n+1} \,\Big|\, (q-1)$$

and using it, show that any divisor $d \,\Big|\, F_n$ of a Fermat number has the form $2^{n+1}k + 1$, for some $k \in \mathbb{N}$. This is similar to the proof of the Theorem about divisors of Mersenne numbers. ***(3 marks)***

(b) Use (a) to list the prime numbers that Euler had to check before he concluded that 641 is the smallest prime divisor of F_5. ***(2 marks)***

4 (i) Prove that there are no primitive Pythagorean triples containing an integer of the form $4k + 2$. ***(3 marks)***

(ii) Consider a sequence $a_0 = 0, a_1 = 1$, $a_{i+1} = 2a_i + a_{i-1}$, for $i \geq 1$, that is

$$0, 1, 2, 5, 12, 29, \ldots$$

Let $A(q)$ be its generating series. Express $A(q)$ as a rational function (quotient of two polynomials in q). ***(6 marks)***

(iii) (a) Find the periodic continued fraction expansion of $\sqrt{40}$. ***(3 marks)***

(b) Using (a) write down two smallest nontrivial solutions of $x^2 - 40y^2 = 1$. ***(3 marks)***

End of Question Paper