The University Of Sheffield.

SCHOOL OF MATHEMATICS AND STATISTICS **Autumn Semester 2013–14**

Topics in Number Theory (Level 3) **2 hours 30 minutes**

Attempt all the questions. The allocation of marks is shown in brackets.

No credit will be given for solutions which rely solely on the use of a calculator. Your solutions should give enough details to make it clear how you arrived at your answers.

1 (i) You publish $(n, e) = (221, 65)$ in the RSA directory and receive 2. Decode it. ***(10 marks)***

(ii) What is the remainder when

$$2013^{2014\times 2015\times 2017}$$

is divided by 13? ***(7 marks)***

(iii) Give the formula for an even perfect number M_p. If $p \equiv 1 \bmod 8$, show that $M_p \equiv 1$ or $3 \bmod 257$. Conversely, if $M_p \equiv 1$ or $3 \bmod 257$, show that $p \equiv 1 \bmod 8$. ***(8 marks)***

2 (i) State the *Law of Quadratic Reciprocity.* ***(2 marks)***

(ii) Solve the congruence

$$x^2 + 9x + 18 \equiv 0 \mod 95.$$ ***(10 marks)***

(iii) Find $\left(\dfrac{98!}{101}\right)$. ***(8 marks)***

(iv) Show that

$$36 \times 27! + 25$$

is divisible by 31. (No credit will be given for a solution that does not use Wilson's Theorem) ***(5 marks)***

3 (i) Expand $\sqrt{17}$ as a continued fraction, find a convergent of $\sqrt{17}$ which differs from it by less that 10^{-6}, and find two solutions of the Pell equation

$$x^2 - 17y^2 = 1.$$

(9 marks)

(ii) Express the continued fraction $[1; 2, 3, 4, \overline{1}]$ in the form $a + b\sqrt{c}$ where a, b are rational numbers and c is a positive integer. ***(7 marks)***

(iii) State Gauss' Lemma and *using it* find $\left(\dfrac{4}{13}\right)$ (no credit will be given without using Gauss' Lemma). ***(5 marks)***

(iv) Let p be a prime number, $\mathbb{F}_p$ be the field with p elements and $\mathbb{X}_p$ be the group of characters of $\mathbb{F}_p$.

(a) For a natural number n such that $n|(p-1)$, define the subgroup $\mathbb{X}_{p,n}$ of $\mathbb{X}_p$. ***(2 marks)***

(b) Using the fact that $\mathbb{X}_p = \{\psi^i \,|\, i = 1, 2, \ldots, p-1\}$ for some character $\psi \in \mathbb{X}_p$ write down all the elements of the set $\mathbb{X}_{p,n}$ via ψ. ***(2 marks)***

4 Let p be a prime number, $\mathbb{F}_p$ be the field with p elements and $\mathbb{F}_p^* = \{g^j \,|\, j = 1, 2, \ldots, p-1\}$ for some $0 \neq g \in \mathbb{F}_p$.

(i) Explain what is meant by saying that χ is a character of the field $\mathbb{F}_p$? ***(2 marks)***

(ii) Is the Legendre symbol $\left(\dfrac{a}{p}\right)$ a character of $\mathbb{F}_p$? Justify your answer. ***(3 marks)***

(iii) Let χ be a character of $\mathbb{F}_p$. Prove that

$$\sum_{a \in \mathbb{F}_p} \chi(a) = \begin{cases} 0 & \text{if } \chi \neq \varepsilon, \\ p & \text{if } \chi = \varepsilon, \end{cases}$$

where ε is the trivial character of $\mathbb{F}_p$. ***(7 marks)***

(iv) Let $\mathbb{X}_p$ be the set of characters of $\mathbb{F}_p$ and $\chi, \psi \in \mathbb{X}_p$.

(a) Define $\chi\psi$ and ψ^{-1}. Prove that $\chi\psi, \psi^{-1} \in \mathbb{X}_p$. ***(6 marks)***

(b) Prove that $\mathbb{X}_p$ is a *cyclic* group of order $p-1$ (You may assume that $\mathbb{X}_p$ is a group). ***(7 marks)***

End of Question Paper