The University Of Sheffield.

SCHOOL OF MATHEMATICS AND STATISTICS **Autumn Semester 2014–15**

Topics in Number Theory **2 hours 30 minutes**

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

Please read the questions carefully. Your solutions should be written legibly and give enough details to make it clear how you arrived at your answers. Usage of calculators is not allowed.

1 (i) What is the remainder when $2014^{2015\times 2017\times 2018}$ is divided by 7? ***(6 marks)***

(ii) You publish $(n, e) = (143, 7)$ in the RSA directory and receive 28. Decode it. ***(9 marks)***

(iii) Use the prime factorization of $n = 375$ to compute $\tau(375)$, $\sigma(375)$, $\mu(375)$ and $\phi(375)$. ***(5 marks)***

(iv) State the *Möbius Inversion Formula* and using it find a simple formula for $s(n) = \sum_{d|n} \mu(d)\tau(\frac{n}{d})$. ***(5 marks)***

2 (i) (a) State *Euler's Theorem* and define what it means for an integer a to be a *primitive root* modulo n. ***(3 marks)***

(b) Show that 3 is a primitive root modulo 17 and that 2 is *not* a primitive root modulo 17. ***(7 marks)***

(ii) How many solutions does the congruence $x^2 \equiv 46 \pmod{137}$ have? (You do not need to find the solutions.) ***(6 marks)***

(iii) Find all solutions of the congruence $x^2 - 4x + 1 \equiv 0 \pmod{23}$. ***(5 marks)***

(iv) State Gauss' Lemma and *using it* find $\left(\frac{5}{11}\right)$ (no credit will be given for a solution not relying on Gauss' Lemma). ***(4 marks)***

3 (i) (a) Define a perfect number. *(2 marks)*

(b) State the theorem about even perfect numbers. *(3 marks)*

(ii) Show that the Mersenne number M_{23} is composite. *(7 marks)*

(iii) Prove that if $n = 2^m + 1$ is prime, then $m = 2^k$. *(5 marks)*

(iv) (a) Give a formula for primitive Pythagorean triples (x, y, z) with even x and $x, y, z > 0$ in terms of two parameters (s, t). *(3 marks)*

(b) Find *all* Pythagorean triples, *not necessarily primitive*, of the form $16, y, z$ $(y, z > 0)$. *(5 marks)*

4 (i) Use a Theorem from the lectures to find $\gcd(u_{21}, u_{35})$ where u_k is the k'th Fibonacci number. *(2 marks)*

(ii) Using induction prove that

$$u_{n+5} \equiv 3u_n \pmod 5.$$

Deduce that u_{715} is divisible by 5. *(5 marks)*

(iii) Express the continued fraction $[2; \overline{1, 3}]$ in the form $a + b\sqrt{c}$ where a, b are rational numbers and c is a positive integer. *(5 marks)*

(iv) (a) Expand $\sqrt{24}$ as a continued fraction. *(5 marks)*

(b) Find the first five convergents $C_k = \dfrac{p_k}{q_k}$. *(4 marks)*

(c) Using the convergents you found find two solutions (x, y), $x, y > 0$ of Pell's equation

$$x^2 - 24y^2 = 1.$$

(4 marks)

End of Question Paper