The University Of Sheffield.

SCHOOL OF MATHEMATICS AND STATISTICS **Autumn Semester 2011–12**

Topics in Number Theory (Level 2) **2 hours**

*Answer **four** questions. If you answer more than four questions, only your best four will be counted.*

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 $(n, e) = (205, 9)$ in the RSA directory and receive 64. Decode it. ***(10 marks)***

(ii) Find two values of the positive integer k, both greater than 1 and one less than 100, such that $n^k \equiv n \pmod{4290}$. ***(9 marks)***

(iii) Verify that $18(34!) + 5!$ is divisible by 37. (No credit will be given for a solution which does not use Wilson's theorem.) ***(6 marks)***

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

(ii) Use the Law of Quadratic Reciprocity to determine whether the congruence

$$2x^2 + 5x - 9 \equiv 0 \pmod{101}$$

has a solution. If it has, solve it. ***(10 marks)***

(iii) Use the Law of Quadratic Reciprocity to prove that, for a prime number $p > 3$,

$$\left(\frac{-3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 6 \\ -1 & \text{if } p \equiv 5 \pmod 6. \end{cases}$$

(6 marks)

(iv) Using part (iii), show that there are infinitely many primes of the form $6k + 1$. ***(7 marks)***

3 (i) State *Gauss' Lemma.* ***(3 marks)***

(ii) Let p be an odd prime number such that $p \equiv 7 \pmod 8$. Prove using Gauss' Lemma that 2 is a quadratic residue modulo p. ***(3 marks)***

Deduce that, if $q > 3$ is a prime number with $q \equiv 3 (\text{mod } 4)$ such that $2q+1$ is also a prime number, then $2^q - 1$ is necessarily composite. ***(5 marks)***

(iii) (a) Define a perfect number. ***(1 mark)***

(b) Prove that, if p is a positive integer such that $2^p - 1$ is prime, then p must be prime. Is the converse true? Justify your answer. ***(5 marks)***

(c) State a formula which gives all even perfect numbers, and prove that every number given by your formula is perfect. You should define any notation you use. ***(8 marks)***

4 (i) State formulae which describe all Pythagorean triples (x, y, z), where the highest common factor of x, y, z is k. ***(3 marks)***

(ii) Determine all Pythagorean triples, not necessarily primitive, which include the number 2012. (Note that 503 is prime.) ***(13 marks)***

(iii) Using Fermat's little theorem prove that for any primitive Pythagorean triple x, y, z the product xyz is divisible by 60. ***(9 marks)***

5 (i) Express $\sqrt{26}$ as a continued fraction and find a convergent of $\sqrt{26}$ which differs from it by less than 10^{-6}. Using your continued fraction, or otherwise, find two solutions of the Pell equation

$$x^2 - 26y^2 = 1$$

in positive integers. ***(13 marks)***

(ii) Let

$$\alpha = \frac{1+\sqrt{5}}{2}, \beta = \frac{1-\sqrt{5}}{2}.$$

(a) The Lucas sequence (ℓ_n) is defined by $\ell_1 = 1, \ell_2 = 3, \ell_n = \ell_{n-1} + \ell_{n-2}$ for $n > 2$. Prove that

$$\ell_n = \alpha^n + \beta^n.$$

(7 marks)

(b) State Binet's formula for the n-th Fibonacci number f_n. ***(3 marks)***

(c) Using parts (a) and (b) prove that $f_n \ell_n = f_{2n}$ for all $n \geq 1$. ***(2 marks)***

End of Question Paper