The University Of Sheffield.

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

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

*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) Given a prime number $p > 3$ and any integer a, prove the congruence

$$a^p(p-1)! \equiv a(p-1) \pmod{1+2+\ldots+(p-1)}.$$

(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 $p \equiv 7 (\text{mod } 8)$. 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) Two positive integers are said to be *amicable numbers* if each is the sum of the proper positive divisors of the other. The prime numbers p, q, r are such that

$$p = 3(2^n) - 1, q = 3(2^{n-1}) - 1, r = 9(2^{2n-1}) - 1,$$

for some integer $n > 1$. Use the result that $\sigma(ab) = \sigma(a)\sigma(b)$ for coprime positive integers a, b to prove that

$$\sigma(2^n pq) = \sigma(2^n r) = 2^n pq + 2^n r.$$

Deduce that $2^n pq$ and $2^n r$ are amicable numbers. ***(14 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) Let $C = [\overline{1;\, 2, 3}\,]$.

(a) Express C in the form $a + b\sqrt{c}$, where a, b are rational numbers and c is a positive integer. ***(7 marks)***

(b) Find a convergent which differs from C by less than 10^{-4}. ***(6 marks)***

(ii) Let n be a positive integer.

(a) Show that $\sqrt{n^2+1} = [n; \overline{2n}]$. ***(6 marks)***

(b) Find two solutions of the Pell equation

$$x^2 - (n^2+1)y^2 = 1$$

in positive integers. ***(6 marks)***

End of Question Paper