The University Of Sheffield.

**SCHOOL OF MATHEMATICS AND STATISTICS** **Autumn Semester 2015–16**

**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) You publish $(n, e) = (133, 7)$ in the RSA directory and receive 81. Decode it. ***(9 marks)***

(ii) Let $p$ be a prime, and let $n = p^3$. Compute $\tau(n)$, $\sigma(n)$, $\mu(n)$, $\phi(n)$. ***(4 marks)***

(iii) State the **Multiplicativity Theorem** and using it find a formula for $F(n) = \sum_{d|n} |\mu(d)|$ in terms of the prime factorization $n = p_1^{k_1} \cdots p_r^{k_r}$. ***(6 marks)***

(iv) Find all primes of the form $4n^4 + 1$. Justify your answer. ***(6 marks)***

**2** (i) (a) Give a definition of order of an element $g$ in a group $G$. ***(2 marks)***

(b) Find orders of $\overline{7}$ and $\overline{2}$ in $\mathbb{Z}_{19}^{\star}$. ***(5 marks)***

(ii) Let $a$ be a primitive root modulo $p$. State the result from the lectures about the order of $a^k$, $k \in \mathbb{N}$. ***(3 marks)***

(iii) Describe explicitly all primes $p$ for which the congruence $x^2 + 5x + 2 \equiv 0 \pmod{p}$ has no solutions. ***(9 marks)***

(iv) State **Euler's Criterion** and using it describe all primes $p$ satisfying the equation $\left(\dfrac{-1}{p}\right) = 1$. ***(6 marks)***

**3** (i) Exhibit a prime divisor for each of the following numbers:

$$2^{14} - 1, \quad 2^{14} + 1.$$

***(4 marks)***

(ii) (a) Give a formula for primitive Pythagorean triples $(x, y, z)$ with even $x$ and $x, y, z > 0$ in terms of two parameters $(s, t)$. ***(2 marks)***

(b) Find *all* Pythagorean triples, *not necessarily primitive*, of the form $20, y, z$ $(y, z > 0)$. ***(6 marks)***

(iii) Show that for any primitive Pythagorean triple $(x, y, z)$, exactly one of the $x$, $y$, $z$ is divisible by 5. ***(7 marks)***

(iv) Show that for $n \geq 2$ the Fermat number $F_n$ has last decimal digit 7.
***(6 marks)***

**4** (i) Show that for any Fibonacci number $u_n$ there are infinitely many Fibonacci numbers divisible by $u_n$. ***(3 marks)***

(ii) (a) Express $\frac{41}{15}$ as a finite continued fraction. ***(5 marks)***

(b) Find the continued fraction representation of $\sqrt{3}$ and compute its convergent $C_4$. ***(7 marks)***

(iii) Find the fundamental solution of Pell's equation

$$x^2 - 7y^2 = 1$$

and then find one more positive solution. ***(5 marks)***

(iv) Let $p > 3$ be a prime. Let us call an element $a \in \mathbb{Z}_p^*$ a **cubic residue** if the equation $x^3 = a$ has a solution in $\mathbb{Z}_p^*$.

Show that if $p \equiv 1 \pmod 3$, then there are two elements of $\mathbb{Z}_p^*$ of order 3 and deduce that $\frac{p-1}{3}$ of the elements $a \in \mathbb{Z}_p^*$ are cubic resides.
***(5 marks)***

## End of Question Paper