The University Of Sheffield.

SCHOOL OF MATHEMATICS AND STATISTICS **Autumn Semester 2017–18**

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.

Please leave this exam paper on your desk
Do not remove it from the hall

Registration number from U-Card (9 digits)
to be completed by student

Blank

1 *(20 marks)*

(i) State Fermat's Little Theorem. *(2 marks)*

(ii) Say what it means for a function to be *multiplicative* and state the Multiplicativity Theorem. *(2 marks)*

(iii) Define a primitive root modulo n. *(2 marks)*

(iv) State Euler's Criterion for quadratic residues. *(2 marks)*

(v) Give the formula for all primitive Pythagorean triples. *(2 marks)*

(vi) State which primes are sums of two integer squares. *(2 marks)*

(vii) Define the Fermat number F_n and state the theorem about the greatest common divisor of two Fermat numbers. *(2 marks)*

(viii) Define the partition function $P(q)$ and give its infinite product expression. *(2 marks)*

(ix) Give the recursive formulas for computing the convergents $C_k = \dfrac{p_k}{q_k}$ of a continued fraction $[a_0; a_1, a_2, \dots]$. *(2 marks)*

(x) What can be said about *odd* perfect numbers? *(2 marks)*

2 *(40 marks)*

(i) What is the remainder when $2016^{2017\times 2018\times 2019}$ is divided by 11? *(5 marks)*

(ii) You publish $(n, e) = (133, 7)$ in the RSA directory and receive 22. Decode it. *(5 marks)*

(iii) Use the prime factorization of $n = 200$ to compute $\tau(n)$, $\sigma(n)$, $\mu(n)$, $\phi(n)$. *(5 marks)*

(iv) How many primitive roots are there in $\mathbb{Z}_{11}^{\star}$? Find one of them. *(5 marks)*

(v) Find a prime divisor for each of $2^{49} - 1$ and $2^{49} + 1$. *(5 marks)*

(vi) Solve the equation $\left(\dfrac{7}{p}\right) = 1$ where p is an odd prime. Give your answer in terms of the remainder of p modulo 28. *(5 marks)*

(vii) Find *all* Pythagorean triples, *not necessarily primitive*, of the form $12, y, z$ $(y, z > 0)$. *(5 marks)*

(viii) 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)*

3 *(24 marks)*

(i) Prove that if $m = x^2 + y^2$ and $n = u^2 + v^2$, where m, n, x, y, u, v are integers, then the product $m \cdot n$ is also a sum of two integer squares. Use the formulas you get to represent $97 \cdot 13$ as a sum of two integer squares. [Hint: use complex numbers.] *(6 marks)*

(ii) (a) Let $H(n) = \sum_{d|n} \frac{1}{d}$. Show that $H(n) = \frac{\sigma(n)}{n}$.

(b) Using (a) show that no divisor of a perfect number is perfect.

(6 marks)

(iii) We are given a sequence $d(n)$ such that its generating series $D(q) = \sum_{n \geq 0} d(n) q^n$ satisfies

$$D(q) = \prod_{k=1}^{\infty} \frac{1}{1 - q^{3k-2}}.$$

Explain the sequence $d(n)$ in terms of partitioning n and compute the term $d(8)$ of the sequence. *(6 marks)*

(iv) Show that for any Pythagorean triple (x, y, z), the product $x \cdot y \cdot z$ is divisible by 15. *(6 marks)*

4 *(16 marks)*

(i) Let p be a prime, and let n be a divisor of $p - 1$.

(a) Find the product of all elements of $\mathbb{Z}_p^\star$ of order n.

(b) Prove that the sum of all elements of $\mathbb{Z}_p^\star$ of order n is equal to $\mu(n)$.

(8 marks)

(ii) We consider the *generalized* Pell's equation $x^2 - dy^2 = a$ where $d > 1$ is square-free and $a \in \mathbb{Z}$, $a \neq 0$ and look for integer solutions $x, y \in \mathbb{Z}$.

(a) Use the $\star$ operation on solutions to show that if an integer solution of a generalized Pell's equation exists, then there are infinitely many solutions.

(b) Show that if $d = p$ is a prime such that $p \equiv 3 \mod 4$ and $a = -1$, then the generalized Pell's equation has no solutions.

(8 marks)

End of Question Paper