The University Of Sheffield.

SCHOOL OF MATHEMATICS AND STATISTICS **Autumn Semester 2018–19**

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) What is the definition of an order of an element g in a finite group G? *(2 marks)*

(ii) State Euler's Theorem. *(2 marks)*

(iii) State the RSA Lemma. *(2 marks)*

(iv) Define the Möbius function $\mu(n)$. *(2 marks)*

(v) Define a quadratic residue modulo n. *(2 marks)*

(vi) Define the Legendre symbol $\left(\frac{a}{p}\right)$, including the conditions on a and p for it to be defined. *(2 marks)*

(vii) How many Pythagorean triples are there? *(2 marks)*

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

(ix) Define a perfect number and state the theorem describing all *even* perfect numbers. *(2 marks)*

(x) Define the group operation $(x, y) \star (x', y')$ on the set of solutions (x, y) of Pell's equation $x^2 - dy^2 = 1$. *(2 marks)*

2 *(42 marks)*

(i) What is the remainder when $2017^{2018\times2019\times2020}$ is divided by 19? *(6 marks)*

(ii) If $n = p_1^{k_1} \cdots p_r^{k_r}$, prove that $\sum_{d|n} |\mu(n)| = 2^r$. *(6 marks)*

(iii) Given that 5 is a primitive root modulo 23 (you do not have to check this), describe explicitly all integers $k > 0$ such that powers 5^k are also primitive roots modulo 23. *(6 marks)*

(iv) Use Gauss reciprocity to decide whether 28 is a quadratic residue modulo 67. *(6 marks)*

(v) Make a guess about the last decimal digit of Fermat numbers F_n and prove your guess. *(6 marks)*

(vi) Find *all* Pythagorean triples, *not necessarily primitive*, of the form $x, 15, z$ $(x, z > 0)$. *(6 marks)*

(vii) Find the periodic continued fraction expansion for $1 + \sqrt{3}$. *(6 marks)*

3 *(28 marks)*

(i) Prove that if $p > 2$ is a prime, then $\mathbb{Z}_{2p}^{\star}$ has a generator. *(7 marks)*

(ii) Let $d(n)$ be the number of ways to represent n as a sum of odd positive integers. For example, $d(5) = 3$ corresponding to 5, 3+1+1, 1+1+1+1+1.

Write down the generating function $D(q)$ for $d(n)$, and *using it* compute the values $d(1), \ldots, d(8)$. *(7 marks)*

(iii) Let $C_n = \dfrac{p_q}{q_n}$ be the convergents of a finite continued fraction. State the p-q relation and prove it. *(7 marks)*

(iv) Prove that for $n > 2$, $\phi(n)$ is even. *(7 marks)*

4 Let d be an integer, p be an odd prime, and let $G_{d,p}$ be the set of $(\overline{x}, \overline{y}) \in \mathbb{Z}_p^2$ satisfying $\overline{x}^2 - \overline{d}\overline{y}^2 = \overline{1}$. In other words, $G_{d,p}$ is the set of solutions of Pell's equation modulo p.

(i) Show that $G_{d,p}$ is a finite abelian group, and compute the order of this group for $p = 5$ and all d. *(6 marks)*

(ii) Show that in general $|G_{d,p}|$ depends only on whether $d \equiv 0 \pmod{p}$, d is a quadratic residue modulo p, or d is a quadratic nonresidue modulo p, and compute $|G_{d,p}|$ in the first two cases. *(4 marks)*

End of Question Paper