JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

2^{nd} YEAR 1^{st} SEMESTER EXAMINATION [**FULL-TIME**]

IIT 3218: INTRODUCTION TO NUMBER THEORY

INSTRUCTION: Attempt question one (**COMPULSORY**) and any other TWO questions only.

QUESTION ONE(*COMPULSORY*) [30 MARKS]

(a). Define a rational number and a prime number. (4 marks)

(b). Describe a good integer. (3 marks)

(c). State the well-ordering axiom. (3 marks)

(d). State the principal of mathematical induction. (4 marks)

(e). Show that there is no rational number whose square is 3. (6 marks)

(f). Define Diophantine equation and hence solve $23x + 29y = 1$. (5 marks)

(g). Determine all positive integers n for which $n + 1|n^2 + 1$. (5 marks)

2 (a). Prove that if $a^k \equiv 1$ mod n, where a is a positive integer $k \leq n$, then a is relatively prime to the positive integer n. (18 marks)

(b). Describe the Legendre symbol as used in number theory. (2 marks)

3 (a). Prove that for all $g \neq 0$ in $\mathbb{Z}_p$, g is such that $g^{p-1} \equiv 1 mod\ p$. (10 marks)

(b). Let $gcd(a, n) = 1$. Prove that for a ϕ-function mapping $\mathbb{N}$ to $\mathbb{C}$, we have $a^{\phi(n)} \equiv 1\ mod\ n$. (10 marks)

4. State and prove the Bachet-Bezout theorem. (20 marks)

5. (a). Prove that every integer greater than one is a product of prime numbers. (18 marks)

(b). State two applications of number theory to computing. (2 marks)