Memorial University of Newfoundland **Fall Semester 2018**
Yorck Sommerhäuser **MATH 3370: Sheet 8**

Introductory Number Theory

Problem 1: A regular polygon of n sides is constructible by straight-edge and compass if and only if $\phi(n)$ is a power of 2. Show that this happens if and only if n is the product of a power of 2 and distinct Fermat primes. (25 points)
(This is a variant of Problem 3 for Chapter 6 in the course notes. It is also stated at the end of Chapter 1.)

Problem 2: Show that $\phi(n) = 14$ is impossible. (25 points)
(This is Problem 6 for Chapter 6 in the course notes.)

Problem 3: Show that $\mathbf{Z}_{pq}^*$, where p and q are distinct odd primes, is not cyclic. [Hint: For $(a, pq) = 1$ prove that $a^{\phi(pq)/2} \equiv 1 \pmod{pq}$.] (25 points)
(This is Problem 20 for Chapter 6 in the course notes. It is not sufficient to cite Theorem 6.5.)

Problem 4: Let p be an odd prime. Prove that a belongs to the exponent 2 modulo p if and only if $a \equiv -1 \pmod{p}$. (25 points)
(This is Problem 21 for Chapter 6 in the course notes.)

Due date: Wednesday, November 14, 2018. Write your solution on letter-sized paper, and write your name on your solution. Write down all necessary computations in full detail, and explain your computations in English, using complete sentences. Prove every assertion that you make in full detail. It is not necessary to copy down the problems again or to submit this sheet with your solution.