Memorial University of Newfoundland **Fall Semester 2020**
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)

Problem 2: Show that $\phi(n) = 14$ is impossible. (25 points)

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 a special case of Theorem 6.5 in Lecture 23, which we did not prove. It is of course not sufficient to cite this theorem.)

Problem 4: Let p be an odd prime. Prove that a has exponent 2 modulo p if and only if $a \equiv -1 \pmod{p}$. (25 points)

Due date: Monday, November 9, 2020. Write your solution on letter-sized paper and send your solution back to me via e-mail. Write down all necessary computations in full detail, and explain your computations in English, using complete sentences. Similarly, prove every assertion that you make in full detail. It is not necessary to copy down the problems again or to write down your student number on your solution.