MATH 418/818, Number Theory and Cryptography, Winter 2022
Homework 3
(Due: February 28 11:59 PM (Kingston time), upload on Crowdmark following question numbers. No extensions can be granted beyond the due date)

Textbook problems.

(1) Exercise 2.13.
(2) Exercise 2.16 (d),(e),(f).
(3) Exercise 2.17.
(4) Exercise 2.18 (b), (d).
(5) Exercise 3.1 (c), (d).
(6) Exercise 3.4 (c).
(7) Exercise 3.6.
(8) Exercise 3.10.
(9) Exercise 3.14.
(10) Exercise 3.15.
(11) Exercise 3.19.
(12) Exercise 3.20.
(13) Exercise 3.22.
(14) Exercise 3.23.

More group theory. For any given element a in a group G, we can check that the set generated by a,

$$< a >= \{a^n : n \in \mathbb{Z}\},$$

forms a subgroup of G, and we call a the generator of the (sub)group $< a >$. This is one of the most obvious ways of finding a (nontrivial) subgroup of a group! In general, if a group H has an element $h \in H$ such that $H =< h >$, we say H is a cyclic group, and call h a generator of H.

(15) Prove that a subgroup of a cyclic group is cyclic. Using this fact, prove that every group of prime order is cyclic.
(16) Let p and q be distinct primes. Find the number of generators of the cyclic group $\mathbb{Z}/pq\mathbb{Z}$.