PROOFS: HOMEWORK 2

ANDREW TSENG: ART2589

Problem 3

Part ai: Subgroups of $Z/5$: $\{0, 1, 4\}$, subgroups of $Z/10$: $\{0, 1, 9\}$

Part aii: Since m is an integer and Z represents the integer set. Given that mZ is the group of integers of multiples of m, then we know that the group does not contain integer a such that:

$$a \mod m > 0$$

Since the group mZ does not contain a, then $mZ \leq Z$.

Part bi: Additive cosets of mZ: $mZ + a$, where:

$$a = \{\ldots, -2m + a, -m + a, a, m + a, 2m + a, \ldots\}$$

In conclusion, the additive cosets of mZ is described as:

$$(mZ + a, +)$$

Part bii: gH is a subgroup of G if the left and right cosets the same. If G is commutative, then the group is an abelian group, which indicates that $gH = Hg$.
Part biii: The union of the cosets of H is G if for all $g \in G$ exists in some coset of H. Since the left coset of H is

$$gH = \{g + h | h \in H\}$$

While the right coset of H is

$$Hg = \{h + g | h \in H\}$$

Part biv:
Part bv:

Problem 4 (1.36):

Part a: If $b \mod p$ is either a perfect square, then the equation:

$$X^2 \equiv b \mod p$$

has two solutions. While if it is not a perfect square, then the equation has no solution.
If $p = 2$, then X always has two solutions because according to Fermet's Little Theorem,

$$X^2 \equiv \begin{cases} 0 & p \mid b \\ 1 & p \nmid b \end{cases}$$

In this case, since $p \nmid b$, then X^2 will always equal 1. Meaning the only solutions to X are -1 and 1.
If $p \mid b$, then X^2 will always only have one solution in 0 because of Fermet's Little Theorem shown above.

Part b:
$(p, b) = (7, 2)$: $\{3\}$, $(p, b) = (11, 5)$: $\{4, 7\}$
$(p, b) = (11, 7)$: $\{\}$ (No square roots), $(p, b) = (37, 3)$: $\{15, 22\}$

Part c:
29 mod 35 has 4 square roots. The reason why this does not contradict the statement in (a) is because 35 is not an odd PRIME integer, which is described as p in part a.

Part d:
Since g is a primitive root, we know that the field consists of the powers of g as shown below:

$$\{1, g, g^2, g^3, \dots, g^{p-2}\}$$

Given $a \equiv g^k \mod p$, we know that a has a square root modulo p if $\sqrt{g^k} \in G$. It is now apparent, that k must be even in order for a to have a square root modulo of p as k being odd leads to $\sqrt{a} \notin G$ as g^k where k is odd is not a a modulo of p.

Problem 5 (2.10):

Part a:
Part b:
Part c: