PROOFS: HOMEWORK 2

ANDREW TSENG: ART2589

Problem 3

Part ai: Subgroups of $Z/5$: $\{0,1,2,3,4\}, \{0\}$ subgroups of $Z/10$: $\{0\}, \{0,1,2,3,4,5,6,7,8,9\}, \{0,5\}, \{2,4,6,8\}$

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:
Let $x \in \bigcup X$ where $X = gH$. This means that $x = gh$ for some $h \in H$ and so $x \in H$ and $x \in G$ follows. However, since $x \in H$, then it is clear that the coset x is in G, thus the union of these cosets is also in G.

Part biv:
Since gH is a set where

$$\{gh | h \in H\}$$

then it is clear that if $g \in G$ then the $H \mapsto gH$. This means $h \mapsto gh$, thus its inverse is a multiplication of g^{-1}. Thus it is clear that the cosets all have the same order thus same size.

Part bv:
Suppose the following:

$$g_1H = \{g_1h_1 | h_1 \in H\}$$
$$g_2H = \{g_2h_2 | h_2 \in H\}$$

There exists a set of $h_1, h_2 \in H$ such that:

$$g_1h_1 = g_2h_2$$

By multipying by h_1^-1:

$$g_1h_1h_1^-1 = g_2h_2h_1^-1$$

It follows that:

$$g_1H = \{(g_2h_2h_1)h_1^{-1} | h_1 \in H\}$$

It becomes clear that the two cosets are either disjoint or equal given that G is the union of all of them annd that $g_1, g_2 \in G$.

Part c:
Since $G = \bigcup(g_iH)$, which was proven in part biii, then the order of G has this relation with the cosets:

$$|G| = \sum i = 1^n |g_iH|$$

Since all cosets have the same order, this means that:

$$\sum i = 1^n |g_iH| = n|H|$$

Which allows us to conclude that the order of G divides the order of H

$$\frac{|G|}{|H|} = n$$

Part d:

Problem 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:
$(p, b) = (7, 2)$: $\{3, 4\}$, $(p, b) = (11, 5)$: $\{4, 7\}$
$(p, b) = (11, 7)$: $\{\}$ (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:

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

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 2.10

Part a:
a and 15619 relate to eachother by this DLP equation:

$$m^{a\alpha} \mod p = m \mod p$$

where $\alpha = 15619$. The explanation for b and 31883 is the same except replace it with $\beta = 31883$.

The algorithm works because Alice first encrypts message m with her key a and Bob encrypts on top of that with b. After sending the encrypted message back to Alice, Alice uses α as explained above to decrypt the message and Bob does the same when he gets the message back. At no point does m show up through the public channel as a result of commutative properties of exponentiation of the same base.

Part b:
Step 1: Bob and Alice agree on a prime integer p.
Step 2. Bob generates a random b as his key, and Alice does so with a.
Step 3: Alice encrypts message m with a and sends $u = m^a \mod p$ to Bob.
Also, Alice and Bob solve for α and β through the DLP equations:

$$g^{a\alpha} \mod p = g \mod p$$

$$g^{b\beta} \mod p = g \mod p$$

Step 4. Bob does the same except encrypts u with his key b. He sends $v = u^b \mod p$ back to Alice.
Step 5: Using α, Alice decrypts v with the equation:

$$w = v^\alpha \mod p$$

and sends w back Bob.
Step 6: Bob does the same except decrypts w with β. Now Bob has solved for m.

Part c:
This cryptosystem has one more exchange than the Elgamal Public Key System, which is more dangerous of getting caught or leaking important numbers. (3 exchanges vs 2 exchanges)

Part d:
Assuming Eve knows that Bob and Alice are using Elgamal and the same for the current cryptosystem, which means the Eve sees and knows exactly what Bob and Alice are exchanging, then she can solve the Elgamal problem and find m with a DLP problem but not the cryptosystem described above. The reason for this is that the Elgamal system publishes p and g prime integers which allows for Eve to solve for m with g^a, c_1, c_2.

Eve can NOT break the system if she can solve the DLP problem because the base value of g is not made public in the described cryptosystem. This makes the solving of m made impossible given m^a, m^b, m^{ab}, p in the 2.10 protocol.

Eve can also not break the