Problem Set II

1. Let a, b, n be positive integers. Consider the modular equation $ax \equiv b \mod n$. Let $d = GCD(a,n)$. Let $S = \{i \in \mathbf{Z}_n : ai \equiv b \mod n\}$ be the set of all solutions of the modular equation. □

   1. Show that S is non-empty if and only if b is a multiple of GCD(a,n).
   2. Show that if $x_0 \in S$, then $x_0 + \frac{n}{d} \in S$.
   3. Show that if $S \neq \emptyset$ then $|S| = d$. (Prove that, if one solution x_0 is found, the others must be $x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, ...$)
   4. For $n = 24$, $b = 9$, find all values of $a \in \mathbf{Z}_n$ for which the equation has a solution.
   5. For $n = 24, a = 15, b = 9$, find all elements in S.
   6. For $n = 24, a = 10$, find all $b \in \mathbf{Z}_n$ for which $S \neq \emptyset$.
   7. For $n = 24, a = 10, b = 14$, find all elements in S.

2. Let n be a positive integer. Let d be a divisor of n. Let $n_1 = \frac{n}{d}$. □

   1. Show that for any i, $1 \leq i \leq n-1$, if $i = i_1 d$ for some i_1 satisfying $1 \leq i_1 \leq n_1$ and GCD$(n_1, i_1) = 1$, then GCD$(n,i) = d$
   2. Show that the cyclic subgroup of $\mathbf{Z}_n$ (with respect to addition $\mod n$) generated by d is the same as the cyclic subgroup generated by kd if and only if GCD$(k, n_1) = 1$.
   3. If j has order n_1 in G, then show that $j = j_1 d$ for some $1 \leq j_1 \leq n_1$ satisfying GCD$(j_1, n_1) = 1$.
   4. Find all elements all elements in $\mathbf{Z}_{24}$ that has order 6. (Use what you proved now, don't start trial and error).

3. Let $(R, +, ., 0, 1)$ be a ring. Show that $R^* = \{a \in R : \exists b \in R, ab = 1\}$ is a group. □

4. Let $(G, ., 1)$ be an Abelian group. Let H be a non-trivial subgroup of G (that is, $\emptyset \neq H \neq G$). For any $x \in G$, let $xH = \{g \in G : \exists h \in H \text{ satisfying } g = xh\}$ (coset of H determined by x). Let $a, b \in G$. For $x, y \in G$, we denote by $xH \oplus yH$ the set $\{xh_1yh_2 : h_1, h_2 \in H\}$. □

   1. Show that if $ab^{-1} \in H$, then $aH = bH$
   2. Show that if $aH = bH$ then $ab^{-1} \in H$.
   3. Show that $aH \oplus bH = abH$.
   4. Show that $|aH| = |bH| = |H|$.
   5. Show that if $aH \neq bH$ then $aH \cap bH = \emptyset$.
   6. Show that if $b = a^{-1}$, then $abH = H$.
   7. Define $\frac{G}{H} = \{aH : a \in G\}$. Thus each element in $\frac{G}{H}$ is a a coset. Show that $(\frac{G}{H}, \oplus, H)$ is a group. (All the ingredients to prove the result has been proven already by the previous questions. One just have to understand what exactly is to be proved!).
   8. For $G = \mathbf{Z}_{24}$, $H = \{0, 6, 12, 18\}$, find the inverse of each element (note that each element here is a coset) in the group $(\frac{G}{H}, \oplus, H)$.

5. Let G be an Abelian group. Let $a, b \in G$. Let $o(a) = m$ and $o(b) = n$, where $o(a)$ and $o(b)$ denote the order of the cyclic subgroups generated by a and b. Consider the set $S(a,b) = \{a^i b^j : i, j \in \mathbf{Z}\}$. Show that $S(a,b)$ is a group. What can you say about the number of elements in the group? □

6. Let g be a generator of a cyclic group of n elements. Let d be a divisor of n. Let $n_1 = \frac{n}{d}$. □

   1. Show that $o(a^d) = n_1$.
   2. Show that for any $1 \leq k \leq n_1$, if GCD$(k, n_1) = 1$, then $o(a^{kd}) = n_1$. This tells us that there are at least $\phi(n_1)$ elements of order n_1 in G (why?).

3. Show that if $o(a^i) = n_1$, then $i = i_1 d$ for some i_1 satisfying GCD$(i_1, n_1) = 1$. This tells us that there are no more elements of order n_1 outside the elements of the form a^{kd} where k satisfies GCD$(k, n_1) = 1$. From the above two cases, we conclude that there are exactly $\phi(n_1)$ elements of order n_1 in G. (You must connect what is proved here with what you have proved in the Q2).
4. Conclude from the above that $\sum_{n_1|n} \phi(n_1) = \sum_{d|n} \phi(d) = n$.

□

7. Let n be any positive integer. Let $x \in \mathbf{Z}_n^*$. Let e be any positive integer such that GCD$(e, \phi(n)) = 1$. Let $y = x^e \mod n$.
    1. Show that there exists a unique positive integer d less than $\phi(n)$ such that $ed \equiv 1 \mod \phi(n)$.
    2. Show that $y^d \equiv x \mod n$. (These equations define the encryption and decryption procedures for message x of a well crypto-system - which one?).