WEEK 8

1. Generalize Proposition 3.4 from the lecture: Given are \( n_1, n_2, \ldots, n_\ell \in \mathbb{Z} - \{0\} \). An integer \( d \) is a greatest common divisor of \( n_1, n_2, \ldots, n_\ell \) just in case that:

   (a) \( d \) is a common divisor of \( n_1, n_2, \ldots, n_\ell \), i.e. \( d \mid n_i \) for each \( i \in \{1, 2, \ldots, \ell\} \);

   (b) if \( d' \) is any other common divisor of \( n_1, n_2, \ldots, n_\ell \) then \( d' \mid d \).

Notice that if \( d \) is a greatest common divisor of \( n_1, n_2, \ldots, n_\ell \) then so is \(-d\). Thus, there are two greatest common divisors of \( n_1, n_2, \ldots, n_\ell \), one is positive and one is negative. The positive one is called the greatest common divisor of \( n_1, n_2, \ldots, n_\ell \) and denoted by \( \gcd(n_1, n_2, \ldots, n_\ell) \). Follow the instructions below to show that \( \gcd(n_1, n_2, \ldots, n_\ell) \) exists:

1. Let

   \[ H = \text{the set of all linear combinations } n_1p_1 + n_2p_2 + \cdots + n_\ell p_\ell \text{ where } p_1, p_2, \ldots, p_\ell \in \mathbb{Z}. \]

   Show that \((H, +)\) is a cyclic group.

2. Let \( d \) be the positive generator of \((H, +)\). Show that \( d \) is the greatest common divisor of \( n_1, n_2, \ldots, n_\ell \).

**Hint.** Follow the proof of Proposition 3.4.

2. Do the problem dual to Problem 1. Given \( n_1, n_2, \ldots, n_\ell \) as in Problem 1, a smallest common multiple is an integer \( n \) such that

   (a) \( n \) is a common multiple of \( n_1, n_2, \ldots, n_\ell \), i.e. \( n \mid n_i \) for each \( i \in \{1, 2, \ldots, \ell\} \);

   (b) if \( n' \) is any other common multiple of \( n_1, n_2, \ldots, n_\ell \) then \( n \mid n' \).

Notice that if \( n \) is a smallest common multiple of \( n_1, n_2, \ldots, n_\ell \) then so is \(-n\). Thus, there are two smallest common multiples of \( n_1, n_2, \ldots, n_\ell \), one is positive and one is negative. The positive one is called the smallest common multiple of \( n_1, n_2, \ldots, n_\ell \) and denoted by \( \text{scm}(n_1, n_2, \ldots, n_\ell) \). Follow the instructions below to show that \( \text{scm}(n_1, n_2, \ldots, n_\ell) \) exists:
1. Let

\[ H = \text{the set of all common multiples of } n_1, n_2, \ldots, n_t. \]

Show that \((H, +)\) is a cyclic group.

2. Let \( n \) be the positive generator of \((H, +)\). Show that \( n \) is the smallest common multiple of \( n_1, n_2, \ldots, n_t \).

\textbf{Hint.} The strategy is similar to that in Problem 1. You just have to amend the parts of the argument so that they will fit with the definition of the smallest common multiple.

3. Let \( p, q \) be two distinct prime numbers. Consider the group \((\mathbb{Z}_{pq}, +_{pq})\). Find all numbers \( n \in \mathbb{Z}_{pq} \) such that \( \langle n \rangle = \mathbb{Z}_{pq} \). How many such numbers are there? Justify your solution by a proof.

\textbf{Hint.} Use Proposition 3.6 and the following fact from number theory: If \( p, q \) are two distinct prime numbers and \( n \mid pq \) then \( n \mid p \) or \( n \mid q \).