Summary on Lecture 10, November 5, 2014 [1]

- **Division algorithm and prime numbers.** Recall that if $m, n \in \mathbf{Z}$, and $m \neq 0$, we say that n *divides* m or m *is divisible by* n iff $m = n \cdot j$, where $j \in \mathbf{Z}$. We can say also that m is a multiple of n. The notation: $n|m$.

  Properties:

  (1) $1|m$ for any $m|0$ for any interger m;
  (2) $(n|m) \wedge (m|k) \Longrightarrow n|k$;
  (3) $(n|m) \wedge (m|n) \Longrightarrow m = \pm n$;
  (4) if $m = c_1 m_1 + \cdots c_s m_s$, and $n|m_i$ for all $i = 1, \ldots, s$, then $n|m$.

  Exercise. Prove (3), (4).

  Recall that p is a prime number if p has no divisors but 1 and itself. We also recall the following fact (see Lecture 5 for the proof):

  Lemma 1. *Let $n \in \mathbf{Z}_+$ be not a prime number. Then there exits a prime p such that $p|n$.*

  We use Lemma 1 to prove the following remarkable fact:

  Theorem 2. *There is infinite number of primes.*

  Proof. Assume there exist only finite number of primes. Let $P = \{p_1, p_2, \ldots, p_k\}$ is the set of all prime numbers, $|P| = k$. Consider the integer: $p_{k+1} = p_1 \cdot p_2 \cdots p_k + 1$. The integer p_{k+1} is either pime or not. If p_{k+1} is not a prime, then by Lemma 1 it has to be divisible by some prime p_j, $j = 1, \ldots, k$, but it is not since the remainder will be 1. Thus p_{k+1} is a prime, and $p_{k+1} \in P$. Then $|P| = k + 1$, not $|P| = k$. This two properties cannot hold together. Contradiction. □

  Division Algorithm. First we prove the existence result.

  Theorem 2. *Let $m, n \in \mathbf{Z}$, and $n \neq 0$. Then there exist unique integers $q \in \mathbf{Z}$ and $r \in \{0, 1, \ldots, n-1\}$ such that $m = n \cdot q + r$.*

  Proof. We consider only the case when $m > 0$ and $n > 0$, leaving the remaining cases to you. If $n|m$, then $m = n \cdot q$ for some $q \in \mathbf{Z}$. If $m = n \cdot q'$, then $n \cdot q - n \cdot q' = 0$, or $n(q - q') = 0$, which implies $q = q'$.

  Let $n \nmid m$ and $n < m$. Then we consider the set

  $$S = \{ \ m - t \cdot n \mid m - t \cdot n > 0 \ \}.$$

  We notice that $S \neq \emptyset$ since $m > n$, i.e., $m - 1 \cdot n > 0$. Also, by definition, all elements of S are positive. By the Well-Ordering Priinciple, there exists a minimal element of S. We denote it by r. We have $m = q \cdot n + r$. We notice that $n > r \geq 0$: indeed, if $r \geq n$, then there is an element $(r - n) = m - (q + 1) \cdot n$ in S. □

  Exercise. Prove uniquness of q and r in the case when $m > n > 0$.

[1] First we discussed the remaining topics from Lecture 9. This is the second part of the lecture