Lecture 30, Nov. 4

30.1 Definition. For $a, b \in \mathbb{Z}$, if $a \neq 0$ and $b \neq 0$ then $lcm(a, b)$ is the smallest $m \in \mathbb{Z}^+$ such that $a \mid m$ and $b \mid m$, and $lcm(a, 0) = lcm(0, a) = 0$.

30.2 Theorem. *Let $a, b \in \mathbb{Z}$. Write*

$$a = \prod_{i=1}^{m} p_i^{k_i}$$

and

$$b = \prod_{i=1}^{m} p_i^{l_i}$$

then

$$gcd(a, b) = \prod_{i=1}^{m} p_o^{min(k_i, l_i)}$$

and

$$lcm(a, b) = \prod_{i=1}^{m} p_o^{max(k_i, l_i)}$$

and

$$gcd(a, b)lcm(a, b) = ab$$

Here ends Chapter 3: Factorization in $\mathbb{Z}$

Chapter 4: Integers Modulo n

Recall that, informally, $\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$ and we add and multiply by adding and multiplying in $\mathbb{Z}$ then finding the remainder after dividing by n.

30.3 Definition (Partition)**.** A partition of a set S is a set P of non-empty disjoint sets whose union is S, that is for all $A \in P$, $A \neq \emptyset$, for all $A, B \in P$, if $A \neq B$ then $A \cap B = \emptyset$ and

$$\bigcup P = \bigcup_{A \in P} A = S$$

or equivalently for all $A \in P$ we have $A \subseteq S$ and for all $a \in S$ we have $a \in A$ for some $A \in P$

30.4 Definition (Equivalence Relation)**.** A equivalence relation on a set S is a binary relation $\sim$ on s such that

1. Reflexivity: for all $a \in S$, $a \sim a$
2. Symmetry: for all $a, b \in S$, if $a \sim b$ then $b \sim a$
3. Transitivity: for all $a, b \in S$, if $a \sim b$ and $b \sim c$ then $a \sim c$

30.5 Definition (Equivalence Class)**.** Given an equivalence relation $\sim$ on a set S, for $a \in S$, the equivalence class of a (in S under $\sim$) is the set

$$[a] = \{x \in S \mid x \sim a\}$$

30.6 Theorem (Equivalence Classes Form a Partition)**.** *Let S be a set. Let $\sim$ be an equivalence relation on S. Then*

1. *for all* $a \in S$ *we have* $a \in [a]$
2. *for all* $a, b \in S$ *we have* $[a] = [b] \Leftrightarrow a \sim b \Leftrightarrow a \in [b] \Leftrightarrow b \in [a]$
3. *for all* $a, b \in S$, *if* $[a] \neq [b]$ *then* $[a] \cap [b] = \emptyset$

It follows that

$$P = \{[a] \mid a \in S\}$$

is a partition of S

Proof. 1. for $a \in S$ we have $a \in [a]$ since $a \sim a$

2. Let $a, b \in S$. Suppose $[a] = [b]$. Then $a \in [a]$ and $[a] = [b]$ so $a \in [b]$ so $a \sim b$. Note that $a \in [b] \Leftrightarrow a \sim b$. Suppose that $a \in [b]$ then $a \sim b$. If $x \in [a]$ then $x \sim a$, so we have $x \sim b$ and so $x \in [b]$. Conversely, if $x \in [b]$ so $x \sim b$ then we have $x \sim a$ and so $x \in [a]$. This shows that $[a] = [b]$
3. Let $a, b \in S$. Suppose $[a] \cap [b] \neq \emptyset$. Choose $c \in [a] \cap [b]$. Since $c \in [a]$ we have $[c] = [a]$. Since $c \in [b]$ we have $[c] = [b]$. Thus $[a] = [c] = [b]$. □

30.7 Definition (Quotient)**.** When $\sim$ is an equivalence relation on S, the partition $p = \{[a] \mid a \in S\}$ is called the quotient of S by $\sim$ and is denoted by $S/\sim$. So we have

$$S/\sim = \{[a] \mid a \in S\}$$

30.8 Example. We construct $\mathbb{Z}$ from $\mathbb{N}$ using a quotient construction.

We define a relation $\sim$ on $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$ by defining $(a, b) \sim (c, d) \Leftrightarrow a + d = b + c$. We check that $\sim$ is an equivalence relation. We define

$$\mathbb{Z} = \mathbb{N}^2/\sim = \{[(a, b)] \mid a \in \mathbb{N},\ b \in \mathbb{N}\}$$

For $n \in \mathbb{N}$ we write

$$n = [(n, 0)] = \{(n, 0), (n + 1, 1), \cdots\}$$
$$-n = [(0, n)] = \{(0, n), (1, n + 1), \cdots\}$$

and we consider $\mathbb{N}$ to be a subset of Z when actually we have an injective map $\phi\colon \mathbb{N} \to \mathbb{Z}$ given by $\phi(n) = n = [(n, 0)]$.

30.9 Example. We construct $\mathbb{Q}$ from $\mathbb{Z}$ as follows. we define $\sim$ on $\mathbb{Z} \times (\mathbb{Z} \times \{0\})$ by $(a, b) \sim (c, d) \Leftrightarrow a + d = b + c$. Then $\mathbb{Q} = (\mathbb{Z} \times (\mathbb{Z} \times \{0\}))/\sim$