**Algebra - I**
**Prof. S. Viswanath & Prof. Amritanshu Prasad**
**Department of Mathematics**
**Indian Institute of Technology, Madras**

# ALGEBRA I

## 1. Lecture 11: Product and Chinese Remainder Theorem

Given two groups $G, H$, $G \times H$ is a group under the operation $(g_1, h_1) \cdot (g_2, h_2) = (g_1 h_1, g_2 h_2)$.

**Example 1.1.** *Consider $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. What is the order? Is it isomorphic to $\mathbb{Z}/4\mathbb{Z}$?*

**Example 1.2.** *Consider $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. It turns out that this group is isomorphic to $\mathbb{Z}/6\mathbb{Z}$.*

This is a special case of very ancient theorem going back to 3rd century China, the Chinese mathematicians Lao Tzu called the Chinese remainder theorem. You have two positive integers $m, n$ whose gcd is 1. So, let us say these are positive integers, and the gcd of m and n is equal to 1. Now, you have this group $\mathbb{Z}/mn\mathbb{Z}$. You have a homomorphism to $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, given by $x \mod mn \to (x \mod m, x \mod n)$. The Chinese remainder theorem says the map is surjective. The way Lao Tzu stated is is that suppose you have two numbers m and n which are co prime, then you can specify what remainder you want modulo m and what remainder you want modulo and find a number which satisfies both these which gives both these remainder simultaneously.

**Example 1.3.** $m = 2, n = 3$*, so if you want remainders* $1, 2$ *in* $\mathbb{Z}/2\mathbb{Z}$ *,* $\mathbb{Z}/3\mathbb{Z}$*. You can just take* $5 \mod 6$*. Another way to solve it is to take* $x \equiv 1 \mod 2$ *so* $x = 2k_1 + 1$ *for some integer* $k_1$*. Which substituted into the second equation gives* $2k_1 + 1 \equiv 2 \mod 3$ *so that* $k_1 \equiv 2 \mod 3$ *since* $2^{-1} = 2$ *(since* $2 \cdot 2 \equiv 1 \mod 3$*). Thus* $k_1 = 3k_2 + 2$ *and* $x = 2(3k_2 + 2) + 1 = 6k_2 + 5$*. Thus* $x \equiv 5 \mod 6$*.*