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

# ALGEBRA I

## 1. Lecture 35: Euclidean domains

Given integers $m, n$ with $m > 0$, there exist integers $q, r$ such that $n = qm + r$, and $0 \leq r < m$. Define $(m, n)$ to be the ideal generated by $m, n$. The Euclidean algorithm gives a way to find their gcd.

**Lemma 1.1.** *Given $n = qm + r$, then $(m, n) = (m, r)$.*

**Example 1.2.** *Let us start with the numbers 168 and 49 ok. So we have*

$$(168, 49) = (49, 21) = (21, 7) = (7).$$

Polynomials also admit Euclidean division. Given polynomials $p(x), h(x)$ then there exist $q(x), r(x)$ such that

$$p(x) = h(x)q(x) + r(x)$$

with $\deg(r) < \deg(h)$.

The Euclidean domain is a ring R which has the following properties.

- Commutative ring.
- Integral domain.
- There exists a size function $d : R \to \mathbb{Z}_{>0}$.
- For all $m, n \in R$, $m \neq 0$, there exist $q, r \in R$ such that $n = qm + r$, where $d(r) < d(m)$ or $r \neq 0$.

An ideal in R is a subset $I \subseteq R$ such that

- $I$ is a group under addition.
- For all $a \in I, rinR$, $ar \in I$.

A principal ideal is of the form $(m)$ for some $m \in R$.

**Theorem 1.3.** *Every ideal in a Euclidean domain is a principal ideal.*

Let us look at one more surprising example of a Euclidean domain: Gaussian integers. The function $d$ is defined by

$$d(a + bi) = a^2 + b^2.$$