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

ALGEBRA I

1. Lecture 37: The fundamental theorem of arithmetic

Developments in the theory of commutative rings have been driven by mainly two areas of mathematical exploration; one has been number theory and the other algebraic geometry. One of the most basic theorems in number theory is the Fundamental Theorem of Arithmetic .

Theorem 1.1 (Fundamental theorem of arithmetic)**.** *Every integer n can be expressed uniquely as*

$$n = p_1^{k_1} \dots p_s^{k_s}$$

for distinct prime numbers $p_1, \dots, p_s$ with exponents $k_i > 0$ for all $i = 1, \dots, s$.

Proof. The proof is by induction. We prove the existence and uniqueness in two steps. For the existence, it is easy to prove for $n = 1$ which is the basic step of the induction. Given an integer n, if n is prime it is true of it so we assume it is composite. Then there must be a prime p that divides n. Then $\frac{n}{p}$ has a prime factorisation by the induction hypothesis. Multiplying both sides by p provides a factorisation of n. For uniqueness we need Bezout's formula: if m and n have gcd equal to d, the ideal generated by m and n is the principal ideal generated by d.

An easy way to prove this is to use Bezout's formula. So, p is a prime number and we want to show that if $p \nmid m, p \nmid n$ then $p \nmid mn$.

Given two factorisations

$$n = p_1 \dots p_r,$$
$$n = q_1 \dots q_s.$$

Then we have each of the primes p_i must divide the second factorisation; thus must belong to the list. Similarly each prime q_i must divide the first factorisation; thus must belong to this list. This proves uniqueness. □