

Lecture 10 (The Integers, Primes and Unique Factorisation)

Last time we showed any pair of integers not both, has a g.c.d. $d = (a, b)$ and the g.c.d. can be expressed as a \mathbb{Z} -linear combination a and b :

$$d = am + bn, \quad m, n \in \mathbb{Z}.$$

Definition 10.1 (Relatively Prime) Integers a and b such that $(a, b) = 1$ are called relatively prime.

Lemma 10.2 Suppose $a|bc$ and $(a, b) = 1$. Then $a|c$.

Proof Since $(a, b) = 1$, we have $1 = ar + bs$ for some $r, s \in \mathbb{Z}$. Hence $c = a(cr) + (bc)s$ is a sum of multiples of a . Hence c is a multiple of a . \square

Definition 10.3 (Prime Number) An integer $p > 1$ is called a prime number if its only positive divisors are 1 and p .

For an integer a and prime p either, $p|a$ and $(a, p) = p$, or $p \nmid a$ and $(a, p) = 1$. A prime number has exactly four divisors in \mathbb{Z} , ± 1 and $\pm p$.

Lemma 10.4 Suppose p is a prime number. Then for integers $a, b \in \mathbb{Z}$, $p|ab$ either $p|a$ or $p|b$.

Proof Sufficient to show that $p|ab$, and $p \nmid a$ implies $p|b$. For a prime number and any $a \in \mathbb{Z}$, either $(a, p) = 1$ or $(a, p) = p$ depending on whether p divides a or not. So $p \nmid a$, $(a, p) = 1$. Hence by Lemma 10.2 if $p|ab$ and $p \nmid a$, $p|b$. \square

Corollary If a prime number p divides a product of integers it divides at least one of the factors in the product.

Proposition 10.5 For $m > 1$, \mathbb{Z}_m is an integral domain if and only if m is prime.

Proof \mathbb{Z} is commutative ring with a unit element. So it is an integral domain if and only if it has no zero divisors.

If m is not prime, $m = ab$, $1 < a, b < m$. Hence in \mathbb{Z}_m , $x = \bar{a} \neq 0$ and $y = \bar{b} \neq 0$ but

$$xy = \bar{a}\bar{b} = \overline{ab} = \bar{0} = 0.$$

So \mathbb{Z}_m has zero divisors if m is not prime.

Suppose $m = p$ is prime. Suppose $xy = 0$ in \mathbb{Z}_m . If $x = \bar{a}$ and $b = \bar{y}$ then $\bar{a}\bar{b} = 0$, i.e. $p|ab$. So by Lemma 10.4 $p|a$ or $p|b$, i.e. $x = 0$ or $y = 0$. So in the case m prime \mathbb{Z}_m has no zero divisors. □

Theorem 10.6 (Unique Factorisation)

(1) Any integer $m > 1$ can be factored as product of primes,

$$a = p_1 p_2 \cdots p_n, \quad n \geq 1, \quad p_1, \dots, p_n \text{ primes.}$$

(2) This factorisation is unique up to order of factors.

Equivalently if

$$a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$$

$m, n \geq 1$, $p_1 \leq p_2 \leq \cdots \leq p_n$, $q_1 \leq q_2 \leq \cdots \leq q_m$ primes, then $m = n$ and $p_1 = q_1, p_2 = q_2, \dots, p_n = q_n$.

Proof

(1) Let $P(m)$ be the proposition that a can be written as product of primes.

We know 2 is prime. So $P(2)$ is true. By mathematical induction to prove $P(m)$ is true for all $m \geq 2$ it is sufficient to show $P(m+1)$ is true if $P(k)$ is true for all $2 \leq k \leq m$.

Assume $P(m)$ is true for all $2 \leq k \leq m$. If $m+1$ is prime we are done. Otherwise $m+1$ is composite $m+1 = bc$, $1 < b, c < m+1$. Then b and c can be written as product of primes by the inductive hypothesis. Hence so can $m+1 = bc$.

(2) We prove uniqueness of factorisation by induction on n

Now suppose

$$p_1 = q_1 q_2 \cdots q_m$$

with p_1 and $q_1 \leq q_2 \leq \cdots \leq q_n$ prime.

Then for any i , $q_i | p_1$ and q_i prime imply $p = q_i$. This is only possible if $m = 1$ and $q_1 = p_1$. So the result is true for $n = 1$.

Assume the result is true for $n \geq 2$. Suppose

$$p_1 p_2 \cdots p_{n+1} = q_1 q_2 \cdots q_m$$

$n \geq 2$, $p_1 \leq p_2 \leq \cdots \leq p_{n+1}$, $q_1 \leq q_2 \leq \cdots \leq q_m$ primes.

Then for some i , $p_{n+1} | q_1 \leq q_m$ and for some j , $q_m | p_j \leq p_{n+1}$. Hence $q_m = p_{n+1}$. Cancelling these factors gives,

$$p_1 p_2 \cdots p_{n+1} = q_1 q_2 \cdots q_{m-1}.$$

By the inductive hypothesis $n = m - 1$ and $p_i = q_i$ for $1 \leq i \leq n$.

We can now conclude $n + 1 = m$ and $p_i = q_i$ for $1 \leq i \leq n + 1$. \square