Discrete Mathematics 2007: Lectures 3 and 4

Integers

Debrup Chakraborty

In these lecture we will learn about some basic properties of integers. Before going further we will need a very important (but obvious) property of non-negative integers which we state next.

> *Well Ordering principle WOP*: Let $\mathbb{N}_0 = \{0, 1, \ldots, \}$ be set of natural numbers. Then every non empty subset $S \subseteq \mathbb{N}_0$ contains a least element.

A least or minimal element of a subset $S \subseteq \mathbb{N}_0$ is an element $s_0 \in S$ for which $s_0 < s$ for all $s \in S$. Similarly, a greatest or maximal element s_0 of S is one for which $s \leq s_0$ for all $s \in S$. Notice that N_0 has a least element 0, but has no greatest element since for each $n \in N_0$, $n + 1 \in N_0$ and $n < n + 1$. It is easy to see that least and greatest elements (if they exist) are always unique.

1 Divisibility

Consider the set of integers $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$. For a and b in $\mathbb{Z}$ we say a divides b or b is divisible by a if there exists $c \in \mathbb{Z}$, such that $b = ac$. We denote this by $a|b$. If a does not divide b we denote it by $a \not| b$.

To begin with we state some simple facts without proofs:

Theorem 1. *For $a, b, c \in \mathbb{Z}$ we have*

1. *$a|a$, $1|a$ and $a|0$*

2. *if* $a|b$ *and* c *is any integer then* $a|bc$

3. *if* $a|b$ *and* $a|c$ *then* $a|(b \pm c)$

4. *if* $a|b$ *and* $b|c$ *then* $a|c$

5. *if* $a|b$ *and* $b|a$ *then* $a = \pm b$

6. $a|b$ *implies* $a| - b$

7. *if* $a|b$ *and* $a|c$*, then for any integers* m, n *we have* $a|(bm + cn)$.

The next theorem that we state is popularly known as the division algorithm.

Theorem 2. *(Division with remainder property) For* a,$b \in \mathbb{Z}$ *with* $b > 0$*, there exist unique* q,$r \in \mathbb{Z}$ *such that* $a = bq + r$ *and* $0 \leq r < b$.

Proof. Consider the set S of non-negative integers of the form $a - zb$ with $z \in \mathbb{Z}$. This set is clearly non-empty, and so contains a minimum. Let r be the smallest integer in this set, with $r = a - qb$ for $q \in \mathbb{Z}$. By definition, we have $r \geq 0$. Also, we must have $r < b$, since otherwise, we would have $0 \leq r - b < r$ and $r - b = a - (q + 1)b \in S$, contradicting the minimality of r. That proves the existence of r and q. To prove uniqueness, suppose that q', r' is a second such pair. Suppose that $r \leq r'$ .By interchanging the pairs if necessary, we can assume that $r \neq r'$. Since $a = qb + r = q'b + r'$, $0 < r' - r = (q - q')b$ .Notice that this means $q' \leq q$ since $b > 0$. If $q > q'$, this implies $b \leq (q - q')d$, hence $b \leq r' - r < b - r \leq b$, and so $b < b$ which is impossible. So $q = q'$ which implies that $r' - r = 0$, contradicting the fact that $0 < r' - r$. So we must indeed have $q' = q$ and $r' = r$. □

We shall write $r = a \bmod b$ that is, $a \mod b$ denotes the remainder in dividing a by b. It is clear that $b|a$ if and only if $a \bmod b = 0$.

2 Greatest Common Divisor

DEFINITION 1. The positive integer c is called the *greatest common divisor* of integers a and b if

1. c is a divisor of a and b.

2. Any divisor of a and b is a divisor of c

We denote the greatest common divisor of a and b by (a, b) or by $gcd(a, b)$.

Theorem 3. *If a and b are integers not both zero, then (a, b) exists; moreover, we can find integers m_0 and n_0 such that $(a, b) = m_0a + n_0b$.*

Proof. Let $\mathcal{M}$ be the set of all integers of the form $ma+nb$, where m and n rang freely over the set of integers. Since at least one of a and b is nonzero so there are nonzero integers in $\mathcal{M}$. Also, if $x = ma + nb \in \mathcal{M}$ then $-x = (-m)a + (-n)b$ is also in $\mathcal{M}$. So $\mathcal{M}$ always have in it some positive integers. As a set of positive integers always have a least element so, the positive integers in $\mathcal{M}$ will also have a least integer. Let c be the smallest positive integer in $\mathcal{M}$. As $c \in \mathcal{M}$, so $c = m_0a + n_0b$ for some $m_0, n_o \in \mathbb{Z}$. We claim that c is (a, b).

To see this, we first observe that if $d|a$ and $d|b$ then $d|(m_0a + n_0b)$, i.e., $d|c$. Now we must show that $c|a$ and $c|b$. Given any element $x \in \mathcal{M}$, by the division algorithm we can say that $x = tc + r$ where $0 \leq r < c$. Now as $x \in \mathcal{M}$ so $x = ma + nb$ for some $m, n \in \mathbb{Z}$. Thus we have $ma + nb = t(m_0a + n_0b) + r$, so $r = (m - tm_0)a + (n - tn_0)b$. Which implies that $r \in \mathcal{M}$. But also $0 \leq r < c$, this forces r to be zero, as c is the smallest nonzero positive element in $\mathcal{M}$. Thus, for any $x \in \mathcal{M}$, $x = tc$, i.e., c divides any element in $\mathcal{M}$. In particular, as $a = 1.a + 0.b \in \mathcal{M}$ and $b = 0.a + 1.b \in \mathcal{M}$, so $c|a$ and $c|b$. This completes the proof of the theorem. □

2.1 Euclids Algorithm

We have proved the existence of the greatest common divisors and established an important property of it, but we still do not know how to find the greatest common divisor of two given integers. We learned such methods in school, here we shall analyze one such method called the Euclids algorithm.

The basic idea of Euclids algorithm is following : If for any integer $b > 0$, $a = bq + r$ where $0 \leq r < b$,using theorem 2. If an integer d divides both b and r, then it also divides a; likewise, if an integer d divides a and b, then it also divides r. From

this observation, it follows that $gcd(a, b) = gcd(b, r)$, and so by performing a division, we reduce the problem of computing $gcd(a, b)$ to the smaller problem of computing $gcd(b, r)$. Now we state Euclids algorithm

Theorem 4. *Let a, b be integers, with $a \geq b \geq 0$. Using the division with remainder property, define the integers $r_0, r_1, \ldots, r_{l+1}$, and $q_1, \ldots, q_l$ where $l \geq 0$, as follows:*

$$\begin{aligned}
a &= r_0 \\
b &= r_1 \\
r_0 &= r_1 q_1 + r_2 \qquad (0 < r_2 < r_1) \\
&\vdots \\
r_{i-1} &= r_i q_i + r_{i+1} \qquad (0 < r_{i+1} < r_i) \\
&\vdots \\
r_{l-2} &= r_{l-1} q_{l-1} + r_l \qquad (0 < r_l < r_{l-1}) \\
r_{l-1} &= r_l q_l \qquad (r_{l+1} = 0)
\end{aligned}$$

Then we have $r_l = gcd(a, b)$.

Proof. For $i = 1, \ldots, l$, we have $r_{i-1} = r_i q_i + r_{i+1}$, from which it follows that the common divisors of r_{i-1} and r_i are the same as the common divisors of r_i and r_{i+1}, and hence $gcd(r_{i-1}, r_i) = gcd(r_i, r_{i+1})$. From this, it follows that $gcd(a, b) = gcd(r_0, r_1) = gcd(r_l, r_{l+1}) = gcd(r_l, 0) = r_l$. □

Example 1. Find g.c.d of $\{1547, 560\}$
$1547 = 2 \times 560 + 427$
$560 = 1 \times 427 + 133$
$427 = 3 \times 133 + 28$
$133 = 4 \times 28 + 21$
$28 = 1 \times 21 + 7$
$21 = 7 \times 3 + 0$
Hence g.c.d.$(1547, 560) = 7$.

According to Theorem 3 (a, b) can be written as a linear combination of a and b. Now

let us try to express 7 as a linear combination of 1547 and 560.

$$\begin{aligned} 7 &= 28 - 1 \times 21 = 28 - 1 \times (133 - 4 \times 28) = 5 \times 28 - 133 \\ &= 5 \times (427 - 3 \times 133) - 133 = 5 \times 427 - 16 \times 133 \\ &= 5 \times 427 - 16 \times (560 - 427) = 21 \times 427 - 16 \times 560 \\ &= 21 \times (1547 - 2 \times 560) - 16 \times 560 \\ &= 21 \times 1547 - 58 \times 560 \end{aligned}$$

Following the method in the above example one can always express the gcd of two numbers as a linear combination of the numbers.

3 Primality

DEFINITION 2. Two integers a and b are called relatively prime if $(a, b) = 1$.

DEFINITION 3. An integer $p > 1$ is a *prime* if its only divisors are ± 1 and $\pm p$.

Lemma 1. *If a is relatively prime to b but $a|bc$, then $a|c$.*

Proof. Since a and b are relatively prime then we can find integers m and n such that $ma + nb = 1$ using Theorem 3 . Thus $mac + nbc = c$. Now $a|mac$ and, it is given $a|nbc$. Hence $a|c$. □

Corollary 1. *If a prime number divides the product of certain integers it must divide at least one of the integers.*

Prime numbers are the building block of the set of integers as it can be seen through *Unique factorization Theorem.*

Theorem 5. *Unique Factorization Theorem: Any positive integer $a > 1$ can be factored in a unique way as $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}$, where $p_1 > p_2 > \dots > p_t$ are prime numbers and where each $\alpha_i > 0$.*

However we will prove this with Mathematical Induction later.

4 Congruence

DEFINITION 4. Let $n > 0$ be a fixed integer. For $a, b \in \mathbb{Z}$ we define $a \equiv b \bmod n$ if $n|(a-b)$. We call this relation as congruence modulo n.

Lemma 2. *1. The relation congruence modulo n defines an equivalence relation on the set of integers.*

2. this equivalence relation has n distinct equivalence classes.

3. If $a \equiv b \bmod n$ and $c \equiv d \bmod n$, then $a + c \equiv b + d \bmod n$ and $ac \equiv bd \bmod n$.

4. If $ab \equiv ac \bmod n$ and a is relatively prime to n, then $b \equiv c \bmod n$.

More generally, if $d = gcd(a, n)$, then $ab \equiv ac \bmod n$ if and only if $b \equiv c \bmod (n/d)$

Proof. 1. First of all we prove that *congruence modulo n* is *equivalence relation.* Since $n|0$ so $n|(a-a)$ which $\Rightarrow a \equiv a \bmod n$ for every a, this proves *reflexivity.* Further if $a \equiv b \bmod n$ then $n|(a-b)$,and so $n|(b-a) = -(a-b)$;thus $b \equiv a \bmod n$, this proves *symmetry.* Finally, if $a \equiv b \bmod n$ and $b \equiv c \bmod n$ then $n|(a-b)$ and $n|(b-c) \Rightarrow n|\{(a-b)+(b-c)\}$, that is , $n|(a-c)$. This is nothing but $a \equiv c \bmod n$, hence transitivity.

2. For any integer a, the collection of all integers b congruent to a modulo n is the congruence class of $a \bmod n$. This is also called the *residue class* of $a \bmod n$, or *equivalence class* of a with respect to the equivalence relation of congruence modulo n. Given an integer a and a modulus n, the equivalence class $\{b \in \mathbb{Z} : b \equiv a \bmod n\} = \{a + nz : z \in \mathbb{Z}\}$ of a modulo n is often denoted by $[a]$; we call it the congruence class of a. By Euclidean algorithm , for any integer a, $a = kn + r$ where $0 \leq r < n$. But then, $a \in [r]$ and so $[a] = [r]$.Thus there are at most n distinct congruence classes; namely $[0], [1], \ldots [n-1]$. These classes are distinct too, for if, $[i] = [j]$ with, say, $0 \leq i < j < n$, then $n|(j-i)$ where $j-i$ is a positive integer less than n, which cannot be possible. Hence we proved second lemma. Thus for fixed n, each equivalence class with respect to congruence modulo n has one and only one representative between 0 and $n-1$. (This is just another way of saying that any integer is congruent modulo n to one and only one integer between 0 and $n-1$).

3. To prove part 3, suppose that $a \equiv c \bmod n$ and $c \equiv d \bmod n$; therefore, $n|(a-b)$ and $n|(c-d) \Rightarrow n|(a-b+c-d) \Rightarrow n|(a+c)-(b+d)$ which proves $(a+c) \equiv (b+d) \bmod n$. In addition $n|(a-b)c+(c-d)b = ac-bd$. Therefore $ac \equiv bd \bmod n$.

4. Finally if $ab \equiv ac \bmod n$ and a is relatively prime to n, then $n|a(b-c)$. Using Lemma 1 we can say $n|(b-c) \Rightarrow b \equiv c \bmod n$.

□

Example 2. Consider the residue classes modulo 6. These are:
$[0] = \{\ldots, -12, -6, 0, 6, 12, \ldots\}$
$[1] = \{\ldots, -11, -5, 1, 7, 13, \ldots\}$
$[2] = \{\ldots, -10, -4, 2, 8, 14, \ldots\}$
$[3] = \{\ldots, -9, -3, 3, 9, 15, \ldots\}$
$[4] = \{\ldots, -8, -2, 4, 10, 16, \ldots\}$
$[5] = \{\ldots, -7, -1, 5, 11, 17, \ldots\}$

We can equip $\mathbb{Z}_n$ with binary operations defining addition and multiplication in a natural way as follows: for a, $b \in \mathbb{Z}$ and $[a]_n$,$[b]_n \in \mathbb{Z}_n$ we define $[a]_n + [b]_n := [a+b]_n$, and we define $[a]_n[b]_n := [ab]_n$.

The set $\mathbb{Z}$ has following interesting properties as given in the next theorem.

Theorem 6. *Let n be a positive integer, and consider the set $\mathbb{Z}_n$ of residue classes modulo n with addition and multiplication of residue classes as defined above. For all $\alpha, \beta, \gamma \in \mathbb{Z}$, we have*

1. $\alpha + \beta = \beta + \alpha$ *(addition is commutative)*
2. $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$ *(addition is associative)*
3. $\alpha + [0]_n = \alpha$ *(existence of additive identity)*
4. $\alpha - \alpha = [0]_n$ *(existence of additive inverses)*
5. $\alpha.\beta = \beta.\alpha$ *(multiplication is commutative)*
6. $(\alpha.\beta).\gamma = \alpha.(\beta.\gamma)$ *(multiplication is associative)*
7. $\alpha.(\beta + \gamma) = \alpha.\beta + \alpha.\gamma$*(multiplication distributes over addition)*

8. $\alpha[1]_n = \alpha$ *(existence of multiplicative identity).*

DEFINITION 5. *Multiplicative Inverse modulo* n: For a positive integer n, and $a \in \mathbb{Z}$, we say that $a' \in \mathbb{Z}$ is a multiplicative inverse of a modulo n if $aa' \equiv 1 \bmod n$.

Theorem 7. *An integer* a *has a multiplicative inverse modulo* n *if and only if* $gcd(a, n) = 1$. *If* $gcd(a, n) = 1$, *let* s *and* t *be integers so that* $sa+tn = 1$. *Then* s *is a multiplicative inverse of* a *modulo* n. *That is,* $s = a'$ *in the definition above.*

Proof. suppose that $gcd(a, n) = 1$. From above, we know that the gcd is expressible as $1 = gcd(a, n) = sa + tn$ for some $s, t \in \mathbb{Z}$. Rearranging this equation, we have $sa = 1 + (-t)m$ which shows that $sa \equiv 1 \bmod n$. Thus, this s is a multiplicative inverse of a modulo n. □