Mathematical Induction & Well Ordering Principle
Unit II

Dr Honey Sharma
GGI, Ludhiana

Well-Ordering Principle

Every non-empty subset of natural numbers contains its least element.

PRINCIPLE OF MATHEMATICAL INDUCTION (WEEK FORM)

Let P (n) be a statement about a positive integer n such that

1. P (1) is true, and
2. P (k + 1) is true whenever one assumes that P (k) is true.

Then P (n) is true for all positive integer n.

Proof. On the contrary, assume that there exists $n_0 \in N$ such that P (n_0) is not true. Now, consider the set $S = \{m \in N : P(m) \text{ is false}\}$.

As $n_0 \in S$, $S = \varnothing$.

So, by Well-Ordering Principle, S must have a least element, say n. By assumption, $n \neq 1$ as P (1) is true. Thus, $n \geq 2$ and hence $n - 1 \in N$.

Therefore, from the assumption that n is the least element in S and S contains all those $m \in N$ for which P (m) is false, one deduces that P $(n - 1)$ holds true as $n - 1 < n$. Thus, the implication "P $(n - 1)$ is true" and Hypothesis 2 imply that P (n) is true. This leads to a contradiction and hence our first assumption that there exists $n_0 \in N$, such that P (n_0) is not true.

Principle of Mathematical Induction

Let P (n) be a statement about a positive integer n such that for some fixed positive integer n_0,

1. P (n0) is true,
2. P (k + 1) is true whenever one assumes that P (k) is true.

Then P (n) is true for all positive integer n $\geq$ n0.

Problems

Prove that for all positive integers n following holds true:

- $\sum n^2 = \frac{n(n+1)(2n+1)}{6}$.
- $n < 2^n$.

Prove that if | S |=n than $|P(s)| = 2^n$.

Prove that $n^3 - n$ is divisible by 3 for all positive integers n.

Prove that $7^{n+2} + 8^{2n+1}$ is divisible by 57 for all positive integers n.

DIVISION ALGORITHM

Let a and b be two integers with $b > 0$. Then there exist unique integers q, r such that

$$a = qb + r, \text{ where } 0 \leq r < b.$$

The integer q is called the quotient and r, the remainder.

Proof: Let $S = \{ a - xb \mid x \in Z, a - xb \geq 0 \}$.

Clearly, for $a>0$, $a \in S$

for $a<0$, $a-ba=-a(b-1)=|a|(b-1)>0$ (as $b>0$) hence $a \in S$.

Hence S is a non-empty subset of N.

Therefore, by Well-Ordering Principle, S has a least element $r = a-bq>0$, for some integer q.

We claim that $r=a-bq<b$.

Lets if possible $a-bq\geq b$,

therefore $a-bq-b\geq 0$ but $a-b(q+1)< a-bq$

which is a contradiction to fact that $r=a-bq$ is least element. Hence our claim is true.

Therefore, integers q, r such that $a = qb + r$ with $0 \leq r < b$.

Uniqueness:

Let (q_1, r_1) and (q_2, r_2) are two such that

$a=bq_1+r_1 = bq_2+r_2$

$b(q_1 - q_2) = r_2 - r_1$

This means b divides $r_2 - r_1$ this is possible only if $r_2 - r_1=0$, $r_2 = r_1$. Hence $q_1 = q_2$.

DIVISIBILITY, PRIMES

- Let a and b be integers with $a \neq 0$. Suppose $b=ca$ for some integer c. We then say that a divides b $(a \mid b)$ or b is divisible by a. We also say that b is a *multiple* of a or that a is a *factor* or *divisor* of b.

- An integer p greater than 1 is called *prime* if the only positive factors of p are 1 and p. A positive integer that is greater than 1 and is not prime is called *composite*.
- ***Remark:*** The integer n is composite if and only if there exists an integer a such that $a \mid n$ and $1 < a < n$.

- Suppose a, b, c are integers. Show that

(i) If $a \mid b$ and $b \mid c$, then $a \mid c$.

(ii) If $a \mid b$ then, for any integer x, $a \mid bx$.

(iii) If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$ and $a \mid (b - c)$.

(v) If $a \mid b$ and $b \mid a$, then $|a| = |b|$, i.e., $a = \pm b$

(vi) If $a \mid 1$, then $a = \pm 1$

- Suppose $a \mid b$ and $a \mid c$. Then, for any integers x and y, $a \mid (bx + cy)$. The expression $bx + cy$ will be called a *linear combination* of b and c.

Theorem : Every integer $n > 1$ can be written as a product of primes.

Proof: The proof is by induction.

If n=2 or n=3 , then is prime, so the statement is true. Now assume that the statement is true for all integers from 2 up to k.

We want to show that this implies k+1 is either prime or a product of primes.

If k+1 is prime then there is nothing to show and we are done.

On the other hand, if k+1 is not prime, then we know there are integers c and d such that $1<c,d<k+1$ (i.e., is divisible by numbers other than 1 and itself), such that k+1=cd. As $1<c,d<k+1$ we know that c and d are either prime or are products of primes. But then k+1 is a product of primes (since the product cd is a product of primes, whether c and d are primes or products of primes themselves).

Hence, by induction result hold for all n.

Theorem: There exists an infinite number of primes.

Proof: We will prove this theorem using a proof by contradiction. We assume that there are only finitely many primes, $p1, p2, \ldots, pn$. Let

$$Q = p1p2 \cdot \cdot \cdot pn + 1.$$

We know that every integer $n > 1$ can be written as a product of primes, therefore Q is prime or else it can be written as the product of two or more primes. However, none of the primes pj divides Q, for if $pj \mid Q$, then pj divides $Q - p1p2 \cdot \cdot \cdot pn = 1$.

Hence, there is a prime not in the list $p1, p2, \ldots, pn$. This prime is either Q, if it is prime, or a prime factor of Q. This is a contradiction because we assumed that

we have listed all the primes. Consequently, there are infinitely many primes.

GREATEST COMMON DIVISOR

- Suppose a and b are integers, not both 0. An integer d is called a *common divisor* of a and b if d divides both a and b, that is, if $d \mid a$ and $d \mid b$.
- Note that 1 is a positive common divisor of a and b, and that any common divisor of a and b cannot be greater than $|a|$ or $|b|$.
- Thus there exists a largest common divisor of a and b; it is denoted by gcd(a, b) and it is called the *greatest common divisor* of a and b.
- The common divisors of 12 and 18 are ±1, ±2, ±3, ±6, gcd(12,18)=6

- A positive integer $d = \gcd(a, b)$ if and only if d has the following two properties:

  (1) d divides both a and b.

  (2) If c divides both a and b, then $c \mid d$.
- For any integer a, we have $\gcd(1, a) = 1$.
- For any prime p, we have $\gcd(p, a) = p$ or $\gcd(p, a) = 1$ according as p does or does not divide a.
- Suppose a is positive. Then $a \mid b$ if and only if $\gcd(a, b) = a$.
- $\gcd(a, b) = \gcd(b, a)$.
- If $x > 0$, then $\gcd(ax, bx) = x \cdot \gcd(a, b)$.

- Relatively Prime Integers

Two integers a and b are said to be relatively prime or coprime if gcd(a, b) = 1.

EXAMPLE

- Observe that: gcd(12, 35) = 1, gcd(49, 18) = 1, gcd (21, 64) = 1, gcd (−28, 45) = 1
- If p and q are distinct primes, then gcd(p, q) = 1.
- For any integer a, we have gcd(a, a + 1) = 1, since any common factor of a and a + 1 must divide their difference (a + 1) − a = 1.

EUCLIDEAN ALGORITHM

LEMMA Let $a = bq + r$, where a, b, q, and r are integers. Then gcd(a, b) = gcd(b, r).

Proof: It is sufficient to show that the common divisors of a and b are the same as the common divisors of b and r.

Suppose that d divides both a and b. Then it follows that d also divides $a - bq = r$. Hence, any common divisor of a and b is also a common divisor of b and r.

Likewise, suppose that d divides both b and r. Then d also divides $bq + r = a$. Hence, any common divisor of b and r is also a common divisor of a and b

Suppose that a and b are positive integers with $a \geq b$. Let $r_0 = a$ and $r_1 = b$. When we successively apply the division algorithm, we obtain

$$r_0 = r_1 q_1 + r_2 \quad 0 \leq r_2 < r_1,$$
$$r_1 = r_2 q_2 + r_3 \quad 0 \leq r_3 < r_2,$$
$$\cdot$$
$$\cdot$$
$$r_{n-2} = r_{n-1} q_{n-1} + r_n \quad 0 \leq r_n < r_{n-1},$$
$$r_{n-1} = r_n q_n.$$

Eventually a remainder of zero occurs in this sequence of successive divisions, because the sequence of remainders $a = r0 > r1 > r2 > \cdots \geq 0$ cannot contain more than a terms. Furthermore, it follows from Lemma that

$$\gcd(a, b) = \gcd(r_0, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-2}, r_{n-1})$$
$$= \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n.$$

Hence, the greatest common divisor is the last nonzero remainder in the sequence of divisions.

Problem: Find the greatest common divisor of 414 and 662 using the Euclidean algorithm.

Solution: Successive uses of the division algorithm give:

$$662 = 414 \cdot 1 + 248$$

$$414 = 248 \cdot 1 + 166$$

$$248 = 166 \cdot 1 + 82$$

$$166 = 82 \cdot 2 + 2$$

$$82 = 2 \cdot 41.$$

Hence, gcd(414, 662) = 2, because 2 is the last nonzero remainder.

LEMMA : If p is a prime and $p \mid a_1 a_2 \cdots a_n$, where each a_i is an integer, then $p \mid a_i$ for some i.

Proof (of the uniqueness of the prime factorization of a positive integer): We will use a

proof by contradiction. Suppose that the positive integer n can be written as the product of primes in two different ways, say, $n = p_1 p_2 \cdots p_s$ and $n = q_1 q_2 \cdots q_t$, each p_i and q_i are primes such that $p_1 \leq p_2 \leq \cdots \leq p_s$ and $q_1 \leq q_2 \leq \cdots \leq q_t$.

When we remove all common primes from the two factorizations, we have

$$pi_1 pi_2 \cdots pi_u = qj_1 qj_2 \cdots qj_v ,$$

where no prime occurs on both sides of this equation and u and v are positive integers. By above Lemma, it follows that pi_1 divides qj_k for some k. Because no prime divides another prime, this is impossible. Consequently, there can be at most one factorization of n into primes in non decreasing order.

- **BÉZOUT'S THEOREM** If a and b are positive integers, then there exist integers s and t such that gcd$(a, b) = sa + tb$

Accordingly, if a and b are relatively prime, then there exist integers x and y such that ax + by = 1.

Express gcd(252, 198) = 18 as a linear combination of 252 and 198.

Solution: To show that $\gcd(252, 198) = 18$, the Euclidean algorithm uses these divisions:

$252 = 1 \cdot 198 + 54$

$198 = 3 \cdot 54 + 36$

$54 = 1 \cdot 36 + 18$

$36 = 2 \cdot 18.$

Using the next-to-last division $18 = 54 - 1 \cdot 36$.

The second division tells us that $36 = 198 - 3 \cdot 54$.

Substituting this expression for 36 into the previous equation,

$18 = 54 - 1 \cdot 36 = 54 - 1 \cdot (198 - 3 \cdot 54) = 4 \cdot 54 - 1 \cdot 198.$

The first division tells us that

$54 = 252 - 1 \cdot 198.$

and hence

$18 = 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198,$

completing the solution.

Theorem: Suppose gcd$(a, b) = 1$, and a and b both divide c. Then ab divides c.

Proof:

If gcd(a,b)=1 then there exist integers s and t such that as+bt=1.

Therefore cas+cbt=c.

As a|c and b|c there exist integers m and n such that c=ma and c=nb.

Hence nbas+mabt= ab(ns+mt)=c.

Hence ab divides c

Theorem: Suppose $a \mid bc$, and gcd$(a, b) = 1$. Then $a \mid c$

Proof: Since gcd$(a, b) = 1$, there exist x and y such that $ax + by = 1$. Multiplying by c yields: $acx + bcy = c$

We have $a \mid acx$. Also, $a \mid bcy$ since, by hypothesis, $a \mid bc$. Hence a divides the sum $acx + bcy = c$.

Corollary : Suppose a prime p divides the product ab. Then $p \mid a$ or $p \mid b$.

THE FUNDAMENTAL THEOREM OF ARITHMETIC

Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of non decreasing size.