DISCRETE MATHEMATICS FOR ENGINEERS
(18MAB302T, UNIT-II)

Outline

What is Combinatorics?

- Combinatorics can loosely be described as the branch of mathematics concerned with selecting, arranging, constructing, classifying, and counting or listing things.
- More specifically, combinatorics deals with counting the number of ways of arranging or choosing objects from a finite set according to certain specified rules.
- Combinatorics is concerned with problems involving the permutations and combinations of certain objects.

Permutation

Definition

An ordered arrangement of r elements of a set containing n distinct elements is called an r-permutation of n elements ($r \leq n$).

- The r-permutation of n elements is denoted by $P(n, r)$ or ${}^{n}P_{r}$ and

$$P(n, r) = {}^{n}P_{r} = \frac{n!}{(n-r)!}.$$

Example

How many ways are there to select a first-prize winner, a second-prize winner, and a third-prize winner from 30 different people who have entered a contest?

Answer: Because it matters which person wins which prize, the number of ways to pick the three prize winners is the number of ordered selections of three elements from a set of 30 elements, that is, the number of 3-permutations of a set of 30 elements. Consequently, the answer is

$$P(30, 3) = {}^{30}P_{3} = \frac{30!}{(30-3)!} = \frac{30!}{27!} = 30 \cdot 29 \cdot 28 = 24360.$$

Combination

Definition

An unordered selection of r elements of a set containing n distinct elements is called an r-combination of n elements ($r \leq n$).

- The r-combination of n elements is denoted by $C(n, r)$ or ${}^{n}C_{r}$ or $\binom{n}{r}$ and

$$C(n, r) = {}^{n}C_{r} = \binom{n}{r} = \frac{n!}{r!(n-r)!}.$$

Example

How many ways are there to select 11 players from a 23-member football squad for a final match?

Answer: The answer is given by the number of 11-combinations of a set with 23 elements. The answer is

$$C(23, 11) = {}^{23}C_{11} = \frac{23!}{11!(23-11)!} = \frac{23!}{11!12!} = 1352078.$$

Addition Rule

Addition Rule: If a task can be done either in one of n_1 ways or in one of n_2 ways, where none of the set of n_1 ways is the same as any of the set of n_2 ways, then there are $n_1 + n_2$ ways to do the task.

Extension of Addition Rule: Suppose that a task can be done in one of n_1 ways, or in one of n_2 ways, $\cdots$,or in one of n_m ways, where none of the set of n_i ways of doing the task is the same as any of the set of n_j ways, for all pairs i and j with $1 \leq i < j \leq m$. Then the number of ways to do the task is $n_1 + n_2 + \cdots + n_m$.

Theorem

When repetition of n elements contained in the set is permitted in r-permutations, then the number of r-permutations is n^r.

Theorem

The number of different permutations of n objects which include n_1 identical objects of type I, n_2 identical objects of type II, $\cdots$ and n_k identical objects of type k is equal to

$$\frac{n!}{n_1!n_2!\cdots n_k!},$$

where $n_1 + n_2 + \cdots + n_k = n$.

Example

Example

Suppose that either a member of the mathematics faculty or a student who is a mathematics major is chosen as a representative to a university committee. How many different choices are there for this representative if there are 37 members of the mathematics faculty and 83 mathematics majors and no one is both a faculty member and a student?

Answer: There are 37 ways to choose a member of the mathematics faculty and there are 83 ways to choose a student who is a mathematics major.

Choosing a member of the mathematics faculty is never the same as choosing a student who is a mathematics major because no one is both a faculty member and a student.

By the sum rule it follows that there are $37 + 83 = 120$ possible ways to pick this representative.

Example

Example

A student can choose a computer project from one of three lists. The three lists contain 23, 15, and 19 possible projects, respectively. No project is on more than one list. How many possible projects are there to choose from?

Answer: The student can choose a project by selecting a project from the first list, or the second list, or the third list.

Because no project is on more than one list, by the sum rule, there are $23 + 15 + 19 = 57$ ways to choose a project.

Example

Example

How many positive integers n can be formed using the digits $3, 4, 4, 5, 5, 6, 7$, if n has to exceed 50,00,000?

Answer: In order that n may be greater than 50,00,000, the first place must be occupied by $5, 6$ or 7.

When 5 occupies the first place, the remaining 6 places are to be occupied by the digits $3, 4, 4, 5, 6, 7$. Thus, number of such numbers$= 6!/2! = 360$ (since the digit 4 occurs twice).

When 6 occupies the first place, the remaining 6 places are to be occupied by the digits $3, 4, 4, 5, 5, 7$. Thus, number of such numbers$= 6!/(2!2!) = 180$ (since 4 and 5 each occurs twice).

When 7 occupies the first place, the remaining 6 places are to be occupied by the digits $3, 4, 4, 5, 5, 6$. Thus, number of such numbers$= 6!/(2!2!) = 180$ (since 4 and 5 each occurs twice).

Therefore, by using addition rule, the number of numbers exceeding 50,00,000 is

$$360 + 180 + 180 = 720.$$

Product Rule

Product Rule: Suppose that a procedure can be broken down into a sequence of two tasks. If there are n_1 ways to do the first task and for each of these ways of doing the first task, there are n_2 ways to do the second task, then there are $n_1 n_2$ ways to do the procedure.

Extension of Product Rule: Suppose that a procedure is carried out by performing the tasks $T_1, T_2, \cdots, T_m$ in sequence. If each task T_i, $i = 1, 2, \cdots, n$, can be done in n_i ways, regardless of how the previous tasks were done, then there are $n_1 n_2 \cdots n_m$ ways to carry out the procedure.

Example

A new company with just two employees, Sanchez and Patel, rents a floor of a building with 12 offices. How many ways are there to assign different offices to these two employees?

Answer: The procedure of assigning offices to these two employees consists of assigning an office to Sanchez, which can be done in 12 ways, then assigning an office to Patel different from the office assigned to Sanchez, which can be done in 11 ways.

By the product rule, there are $12 \times 11 = 132$ ways to assign offices to these two employees.

Example

Example

From a club consisting of 6 men and 7 women, in how many ways can we select a committee of
(i) 3 men and 4 women?
(ii) 4 persons which has at least 1 women?

Answer of (i): 3 men can be selected form 6 men in ${}^6C_3$ ways.

4 women can be selected form 7 women in ${}^7C_4$ ways.

Therefore, by using product rule, the committee of 3 men and 4 women can be selected by

$$ {}^6C_3 \times {}^7C_4 = 20 \times 35 = 700. $$

Answer of (ii): For the committee to have at least 1 woman, we have to select 3 men and 1 woman or 2 men and 2 women or 1 man and 3 women or no man and 4 women.

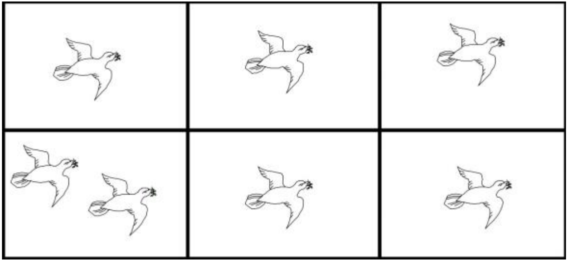
The selection can be done in

$$ \begin{aligned} & ({}^6C_3 \times {}^7C_1) + ({}^6C_2 \times {}^7C_2) + ({}^6C_1 \times {}^7C_3) + ({}^6C_0 \times {}^7C_4) \\ = \ & (20 \times 7) + (15 \times 21) + (6 \times 35) + (1 \times 35) \\ = \ & 140 + 315 + 210 + 35 \\ = \ & 700. \end{aligned} $$

Pigeonhole Principle

Pigeonhole Principle: If n pigeons are accommodated in m pigeonholes and $n > m$ then at least one pigeonhole will contain two or more pigeons.

Equivalently, if n objects are put in m boxes and $n > m$, then at least one box will contain two or more objects.



Generalization of the Pigeonhole Principle: If n pigeons are accommodated in m pigeonholes and $n > m$ then one of the pigeonholes must contain at least $\left\lfloor \frac{n-1}{m} \right\rfloor + 1$ pigeons, where $\lfloor x \rfloor$ denotes the greatest integer less than or equal to x, which is a real number.

Examples (Pigeonhole Principle)

- Among any group of 367 people, there must be at least two with the same birthday, because there are only 366 possible birthdays.
  - Pigeon = 367 people
  - Pigeonholes = 366 birthdays.

  Note: Is there a pair of you with the same birthday date? YES, since there are more than 366 of you.
- In any group of 27 English words, there must be at least two that begin with the same letter, because there are 26 letters in the English alphabet.
  - Pigeon = 27 words,
  - Pigeonholes = 26 alphabet.
- Is it true that within a group of 700 people, there must be 2 who have the same first and last initials?
  Note that, there are $26^2 = 676$ different sets of first and last initials and we have 700 people.
  - Pigeon = 700 people,
  - Pigeonholes = 676 different sets of first and last initials.

  Answer: YES.

Examples (Generalization of the Pigeonhole Principle)

- If there are 105 of you, are there at least 3 of you with the same birthday week? Note that, there are 52 weeks in a year.
  - Pigeon (n) = 105 people,
  - Pigeonholes (m)= 52 week.

  By using Generalization of the Pigeonhole Principle, we can say at least $\left\lfloor \frac{105-1}{52} \right\rfloor + 1 = 3$ people is having same birthday week.

  Answer: YES.

- What is the minimum number of students required in a Discrete Mathematics class to be sure that at least six will receive the same grade, if there are five possible grades, A, B, C, D, and F?
  Answer: Suppose, there is N number of students in the Discrete Mathematics class.
  - Pigeon (n) = N students,
  - Pigeonholes (m)= 5 grades.

  By using Generalization of the Pigeonhole Principle, we can write

  $$\left\lfloor \frac{N-1}{5} \right\rfloor + 1 = 6 \Rightarrow \left\lfloor \frac{N-1}{5} \right\rfloor = 5 \Rightarrow 5 \leq \frac{N-1}{5} < 6 \Rightarrow 26 \leq N < 31.$$

  Therefore, at least $N = 26$ students required in a Discrete Mathematics class to be sure that at least six will receive the same grade, if there are five possible grades, A, B, C, D, and F.

Principle of Inclusion and Exclusion

Principle of Inclusion and Exclusion: If A and B are finite subset of universal set U, then

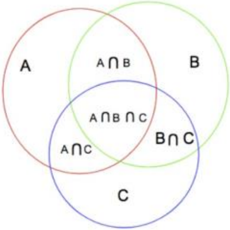
$$|A \cup B| = |A| + |B| - |A \cap B|,$$

where, $|A|$ denotes the cardinality of the set A (i.e. the number of elements in A).

This principle can be extended to a finite number of finite sets $A_1, A_2, \cdots, A_n$ as follows

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_i |A_i| - \sum_{i<j} |A_i \cap A_j| + \sum_{i<j<k} |A_i \cap A_j \cap A_k| + (-1)^{n+1} |A_1 \cap A_2 \cap \cdots \cap A_n|,$$

where, the first sum is over all i, the second sum is over all pairs i, j with $i < j$, the third sum is over all triples i, j, k with $i < j < k$ and so on.



$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

Example

Example

How many binary strings of length 8 either start with a “1” bit or end with two bits “00”?

Answer: If the binary string starts with “1”, then, there are 7 characters left which can be filled in $2^7 = 128$ ways.

If the binary string ends with “00” then 6 characters can be filled in $2^6 = 64$ ways.

Now, if we add the above sets of ways and conclude that it is the final answer, then it would be wrong.

This is because there are binary strings, start with “1” and end with “00” both, and since they satisfy both criteria they are counted twice.

So we need to subtract such binary strings to get a correct count.

Binary strings that start with “1” and end with “00” have five characters that can be filled in $2^5 = 32$ ways.

So, by the inclusion and exclusion principle, we get:

$$\text{Total binary strings} = 128 + 64 - 32 = 160.$$

Divisibility

Definition

When a and b are two integers with $a \neq 0$, a is said to divide b (i.e., we can say that a divides b or b is divisible by a), if there is an integer c such that $b = ac$ and it is denoted by the notation $a \mid b$.

When a divides b, a is called a divisor or factor of b and b is called a multiple of a.

Note

i) When a divides b, then $-a$ also divides b, since $b = ac$ can be written as $b = (-a)(-c)$.

ii) If a does not divide b, then it is denoted by $a \nmid b$.

iii) The relation "a divides b" is a reflexive and transitive in the set of positive integers but not symmetric.

Theorem

Let a, b, $c \in z$, the set of integers. Then

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

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

(iii) If $a \mid b$, then $a \mid mb$, for any integer m.

(iv) If $a \mid b$and $a \mid c$, then $a \mid (mb + nc)$, for any integers m and n.

Proof:

(i) Since $a \mid b$and $a \mid c$, it follows, from definition of divisibility, that $b = ma$ and $c = na$, where m and n are integers.
Hence $b + c = (m + n)a$.
This means that a divides $(b + c)$ or $a \mid (b + c)$.
(ii) Since $a \mid b$and $b \mid c$, we have $b = ma$ and $c = nb$, where m and n are integers.
Hence $c = n(ma) = (mn)a$.
This means that a divides c or $a \mid c$.
(iii) Since $a \mid b$, we have $b = na$.
Hence $mb = (mn)a$, where m and n are integers. This means that a divides mb or $a \mid mb$.
(iv) We can prove by using (i) and (iii).

Prime numbers

Definition

A positive integer $p > 1$ is called prime, if the only positive factors of p are 1 and p. A positive integer > 1 and is not prime is called composite.

Note

i) The positive integer 1 is neither prime nor composite.
ii) The positive integer n is composite, if there exists positive integers a and $b$such that $n = ab$, where $1 < a, b < n$.
iii) A number that is not a prime is divisible by prime.

Fundamental Theorem of Arithmetic

Theorem

Every integer $n > 1$ can be written uniquely as a product of prime numbers.

Proof

We shall prove the theorem by introduction.
Let $n = 2$.
Since 2 is prime, $n (= 2)$ is a product of primes (as a product may consist of a single factor).
Let $n > 2$.
If n is prime, it is a product of primes, i.e., a single factor product.
If n is not prime, i.e., composite, let us assume that the theorem holds good for positive integers less than n and that $n = ab$. Since $a, b < n$, each of a and $b$can be expressed as the product of primes (by the assumption).
Hence, $n = ab$ is also a product of primes.

Theorem

For prime p and integers a and b, if $p \mid ab$, then either $p \mid a$ or $p \mid b$.
Hint: If $p \mid ab$ but $p \nmid a$, then $p \mid b$.

Theorem

If p is a prime and $p \mid a_1 a_2 \cdots a_n$, then either $p \mid a_1$ or $p \mid a_2$ or $\cdots$ or $p \mid a_n$.
Proof: We will prove this by mathematical induction.
For $n = 2$ the above statement is true (by previous theorem).
For $n > 2$, let $a = a_1$ and $b = a_2 a_3 \cdots a_n$, then either $p \mid a \ (= a_1)$ or $p \mid b \ (= a_2 a_3 \cdots a_n)$.
If $p \nmid a_1$, then similarly we will get either $p \mid a_2$ or $p \mid a_3 a_4 \cdots a_n$.
Finally we can conclude that if $p \mid a_1 a_2 \cdots a_n$, then either $p \mid a_1$ or $p \mid a_2$ or $\cdots$ or $p \mid a_n$.

Finding prime factorization of a given number

Prime factorization

The unique expression for the integer $n > 1$ as a product of primes is called the prime factorization or prime decomposition of n.

Note

If there be k_i prime factors of n, each equal to p_i, where $1 \leq i \leq r$, then n can be written as
$n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_r^{k_r}$.

Example

If $n = 120$, then $120 = 2^3 \times 3^1 \times 5^1$. Here $p_1 = 2$, $p_2 = 3$ and $p_3 = 5$; $k_1 = 3$, $k_2 = 1$ and $k_3 = 1$.

Example

Find the prime factorization of 7007.

Solution: To find the prime factorization of 7007, first perform divisions of 7007 by successive primes, beginning with 2. None of the primes 2, 3, and 5 divides 7007. However, 7 divides 7007, with $7007/7 = 1001$. Next, divide 1001 by successive primes, beginning with 7.

It is immediately seen that 7 also divides 1001, because $1001/7 = 143$. Continue by dividing 143 by successive primes, beginning with 7. Although 7 does not divide 143, 11 does divide 143, and $143/11 = 13$. Because 13 is prime, the procedure is completed. It follows that

$7007 = 7 \cdot 1001 = 7 \cdot 7 \cdot 143 = 7 \cdot 7 \cdot 11 \cdot 13$. Consequently, the prime factorization of 7007 is $7 \cdot 7 \cdot 11 \cdot 13 = 7^2 \cdot 11 \cdot 13$.

Theorem

The number of prime numbers is infinite.

Proof: We will prove this theorem using a proof by contradiction. We assume that there are only finitely many primes, $p_1, p_2, \ldots, p_n$.
Let $Q = p_1p_2 \ldots p_n + 1$. By the fundamental theorem of arithmetic, Q is prime or else it can be written as the product of two or more primes. However, none of the primes p_j divides Q, for if $p_j \mid Q$, then p_j divides $Q - p_1p_2 \ldots p_n + 1$. Hence, there is a prime not in the list p_1, $p_2, \ldots, p_n$. 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.

Theorem: If n >1 is a composite integer and p is a prime factor of n, then p ≤ $\sqrt{n}$.

Proof: If n>1 is composite, by the definition of a composite integer, we know that it has a factor 'a ' with 1 < a ≤ b< n. Hence, by the definition of a factor of a positive integer, we have n = ab, where b is a positive integer greater than 1.

We will show that a ≤ $\sqrt{n}$ or b≤ $\sqrt{n}$. If a > $\sqrt{n}$ and b > $\sqrt{n}$, then ab > $\sqrt{n}$. $\sqrt{n}$ = n, which is a contradiction. Because both a and b are divisors of n, we see that n has a positive divisor not exceeding √ n. This divisor is either prime or, by the fundamental theorem of arithmetic, has a prime divisor less than itself. In either case, n has a prime divisor less than or equal to √ n. Note To test if a given integer n is prime, it is enough to see that it is not divisible by any prime less than or equal to √ n.

As an example, to test the primability of 101, we check it is divisible be the prime number less than or equal to 101, namely, 2, 3, 5 and 7. Since 101 is not divisible by any of these prime number, 101 is a prime number.

The Division Algorithm

The Division Algorithm

Let a be an integer and b a positive integer. Then there are unique integers q and r, with $0 \leq r < d$, such that $a = bq + r$. The integers q and r are respectively called the quotient and the remainder when a is divided by b.

Example

If $a = 46$, $b = 13$, then $q = 3$ and $r = 7$. Here $46 = 13(3) + 7$.

GCD

Definition

Let a and $b$be integers, not both zero. The largest integer d such that $d \mid a$ and $d \mid b$is called the greatest common divisor of a and b. The greatest common divisor of a and $b$is denoted by gcd(a, b).

The greatest common divisor of two integers, not both zero, exists because the set of common divisors of these integers is nonempty and finite. One way to find the greatest common divisor of two integers is to find all the positive common divisors of both integers and then take the largest divisor.

Example

What is the greatest common divisor of 24 and 36?

Solution: The positive common divisors of 24 and 36 are 1, 2, 3, 4, 6, and 12. Hence, gcd(24, 36) = 12.

Definition

The integers a and b are relatively prime if their greatest common divisor is 1.

It follows from the definition that the integers 17 and 22 are relatively prime, because gcd(17, 22) = 1.

Another way to find the greatest common divisor of two positive integers is to use the prime factorizations of these integers. Suppose that the prime factorizations of the positive integers a and b are
$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$, $b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$,
where each exponent is a nonnegative integer, and where all primes occurring in the prime factorization of either a or b are included in both factorizations, with zero exponents if necessary. Then gcd(a, b) is given by
$\gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)}$,
where $\min(x, y)$ represents the minimum of the two numbers x and y.

Because the prime factorizations of 120 and 500 are $120 = 2^3 \cdot 3 \cdot 5$ and $500 = 2^2 \cdot 5^3$, the greatest common divisor is
$\gcd(120, 500) = 2^{\min(3,2)} 3^{\min(1,0)} 5^{\min(1,3)} = 2^2 3^0 5^1 = 20$.

The Euclidean Algorithm

Lemma

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

The Euclidean Algorithm

Statement: When a and b are two integers ($a > b$), if r_1 is the remainder when a is divided by b, r_2 is the remainder when b is divided by r_1, r_3 is the remainder when r_1 is divided by r_2 and so on and if $r_{k+1} = 0$, then the last non-zero remainder r_k is the $\gcd(a, b)$

Example

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.

Theorem

$\gcd(a, b)$ can be expressed as an integral linear combination of a and b. i.e., $\gcd(a, b) = ma + nb$, where m and n are integers.

Example

For example, we consider the steps we used to find the $\gcd(414, 662)$ that are given below: $662 = 414 \cdot 1 + 248$

$414 = 248 \cdot 1 + 166$

$248 = 166 \cdot 1 + 82$

$166 = 82 \cdot 2 + 2$

From the last equation we have

$$\begin{aligned}
2 &= 166 - 82 \cdot 2 \\
&= 166 - (248 - 166 \cdot 1) \cdot 2 \\
&= 166 \cdot 3 - 248 \cdot 2 \\
&= (414 - 248) \cdot 3 - 248 \cdot 2 \\
&= 414 \cdot 3 - 248 \cdot 5 \\
&= 414 \cdot 3 - (662 - 414 \cdot 1) \cdot 5 \\
&= 414 \cdot 8 - 662 \cdot 5
\end{aligned}$$

Properties of gcd

(i) If $c \mid ab$ and a and c are co-prime, then $c \mid b$.

(ii) If a and $b$are co-prime and a and c are co-prime, then a and bc are co-prime.

(iii) If a and b are integers, which are not simultaneously zero, and k is a positive integer, then

$$\gcd(ka, kb) = k \gcd(a, b).$$

(iv) If $\gcd(a, b) = d$, $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

(v) If $\gcd(a, b) = 1$, then for any integer c, $\gcd(ac, b) = \gcd(c, b)$.

(vi) If each of $a_1, a_2, \ldots, a_n$ is co-prime to b, then the product $(a_1 a_2 \cdots a_n)$ is also co-prime to b.

LCM

Definition

The least common multiple of the positive integers a and $b$is the smallest positive integer that is divisible by both a and b. The least common multiple of a and b is denoted by $\text{lcm}(a, b)$.

The least common multiple exists because the set of integers divisible by both a and $b$is nonempty (because ab belongs to this set, for instance), and every nonempty set of positive integers has a least element. Suppose that the prime factorizations of a and b are as before. Then the least common multiple of a and b is given by

$$\text{lcm}(a, b) = p_1^{\max(a_1,\, b_1)} p_2^{\max(a_2,\, b_2)} \cdots p_n^{\max(a_n,\, b_n)},$$

where $\max(x, y)$ represents the maximum of the two numbers x and y.

Example

What is the least common multiple of $2^3 3^5 7^2$ and $2^4 3^3$?

Solution: $\text{lcm}(2^3 3^5 7^2, 2^4 3^3) = 2^{\max(3,4)} 3^{\max(5,3)} 7^{\max(2,0)} = 2^4 3^5 7^2$.

Theorem

Let a and b be positive integers. Then $ab = \gcd(a, b) \cdot \mathrm{lcm}(a, b)$.

Proof: Let the prime factorization of a and b be
$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ and $b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$.
Then $\gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)}$
and $\mathrm{lcm}(a, b) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \cdots p_n^{\max(a_n, b_n)}$
We observed that if $\min(a_i, b_i)$ is a_i (or b_i) then $\max(a_i, b_i)$ is b_i (or a_i), $i = 1, 2, \ldots, n$.
Hence,

$$
\begin{aligned}
& \gcd(a, b) \times \mathrm{lcm}(a, b) \\
&= p_1^{\min(a_1,b_1)+\max(a_1,b_1)} \cdot p_2^{\min(a_2,b_2)+\max(a_2,b_2)} \cdots p_n^{\min(a_n,b_n)+\max(a_n,b_n)} \\
&= p_1^{(a_1+b_1)} \cdot p_2^{(a_2+b_2)} \cdots p_n^{(a_n+b_n)} \\
&= (p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n})(p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}) \\
&= ab
\end{aligned}
$$

Example

Using prime factorization, find the gcd and lcm of (231, 1575) verify also that $\gcd(m, n) \cdot \operatorname{lcm}(m, n) = mn$.

Solution: $231 = 3^1 \cdot 5^0 \cdot 7^1 \cdot 11^1$, $1575 = 3^2 \cdot 5^2 \cdot 7^1 \cdot 11^0$

Now

$$\begin{aligned} \gcd(231, 1575) &= 3^{\min(1,\ 2)} \times 5^{\min(0,\ 2)} \times 7^{\min(1,\ 1)} \times 11^{\min(0,\ 1)} \\ &= 3^1 \cdot 5^0 \cdot 7^1 \cdot 11^0 = 21. \end{aligned}$$

$$\begin{aligned} \operatorname{lcm}(231, 1575) &= 3^{\max(1,\ 2)} \times 5^{\max(0,\ 2)} \times 7^{\max(1,\ 1)} \times 11^{\max(0,\ 1)} \\ &= 3^2 \cdot 5^2 \cdot 7^1 \cdot 11^1 = 17325. \end{aligned}$$

$$\begin{aligned} \gcd(231, 1575) \cdot \operatorname{lcm}(231, 1575) &= 21 \times 17325 \\ &= 363825 \\ &= 231 \times 1575 \text{ (verified)}. \end{aligned}$$

Example

Use Euclidean algorithm to find gcd(1819, 3587) and express the gcd as a linear combination of the given numbers.
Solution: By division algorithm,

$$\begin{aligned}
3587 &= 1 \cdot 1819 + 1768 \\
1819 &= 1 \cdot 1768 + 51 \\
1768 &= 34 \cdot 51 + 34 \\
51 &= 1 \cdot 34 + 17 \\
34 &= 2 \cdot 17 + 0
\end{aligned}$$

Since the last non-zero remainder is 17, gcd(1819, 3587) = 17.
Now

$$\begin{aligned}
17 &= 51 - 1 \cdot 34 \\
&= 51 - 1 \cdot (1768 - 34 \cdot 51) \\
&= 35 \cdot 51 - 1 \cdot 1768 \\
&= 35 \cdot (1819 - 1 \cdot 1768) - 1 \cdot 1768 \\
&= 35 \cdot 1819 - 36 \cdot 1768 \\
&= 35 \cdot 1819 - 36 \cdot (3587 - 1 \cdot 1819) \\
&= 71 \cdot 1819 - 36 \cdot 3587
\end{aligned}$$