# 4.3 - PRIMES AND GCD

## 4.3(A) PRIME:

An integer P greater than 1 is called Prime if the only positive factors of P are 1 and P.

Every integer greater than 1 is divisible by at least two integers, because a positive integer is divisible by 1 and by itself.

> Positive Integers that have exactly two different positive integer factors are called primes

### COMPOSITE:

A positive inter that is greater than 1 and is not Prime is called Composite.

An inter n is composite iff there exists an integer a such that $a|n$ and $1<a<n$.

**NOTE**

The integer 1 is not prime, because it has only one +ve factor.

Example :

- The integer 7 is prime : its only positive factors are 1 and 7.
- The integer 9 is composite: it is divisible by 3

THE PRIMES ARE BUILDING BLOCKS OF POSITIVE INTEGERS.

### The Fundamental Theorem of Arithmetic

Every integer (greater than 1) canbe writen 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.

**APPLICATION:**

In Cryptology, Large primes are used in some methods for making messages secret.

**Example:**

The prime factorization of 100, 641, 999 & 1024.

**Sol:-**

As every integer greater than 1 can be written uniquely as prime or as the product of two or more primes, so

- 100 can be written as

$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$ (prime factorization of 100)

| | |
|---|---|
| 2 | 100 |
| 2 | 50 |
| 5 | 25 |
| | 5 |

$641 = 641$

$999 = 3 \cdot 3 \cdot 3 \cdot 37$

| | |
|---|---|
| 3 | 999 |
| 3 | 333 |
| 3 | 111 |
| | 37 |

$1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}$

## HOW CAN WE FIND THAT A NUMBER IS PRIME?

It is often to show that a given integer is prime.
One procedure for showing that an integer is prime is based on the following observation.

**THEOREM:**

If n is composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.

**Proof:**

- As given n is composite, then by definition of Composite
  there exists an integer a such that $a|n$ and $1<a<n$.
- As $a|n$, then by the definition of divisibility,
  n is a multiple of a for some $b \in Z^+$ (Also, $1<b<n$)

~~Here both a and b are~~

i.e $n = ab$ for some $b \in Z^+$

Here both a and b are divisors of n.

**TO SHOW:**

n has a prime divisor less than or equal to $\sqrt{n}$

i.e $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$ : both are divisors of n

We use Contradiction to show that $a \leq \sqrt{n}$ or $a \leq \sqrt{n}$

Suppose

$$a > \sqrt{n} \text{ and } a > \sqrt{n}$$

$$\Rightarrow ab > \sqrt{n} \cdot \sqrt{n}$$

$$ab > n$$

which is Contradiction as n is Composite and has the form $n = ab$

Consequently,

$$a \leq \sqrt{n} \quad \text{or} \quad b \leq \sqrt{n}$$

As $d \mid n$, and we Know that Every number can be written as product of primes. So, a is prime diviso

Because both a and b are positive divisors of n not exceeding $\sqrt{n}$ and by the theorem (fundamental theorem of arithmetic),

this divisor (i.e a) is either prime or has a prime divisor.

So, we can say that (it is proved),

n has a prime divisor less than or equal to $\sqrt{n}$

Now, we can show that

An integer is prime if it is not divisible by any prime less than or equal to its square root.

This leads to the brute-force algorithm known as **TRIAL DIVISION** to find whether the given integer is prime or not.

**TRIAL DIVISION**

To show whether n is prime,
we divide n by all primes not exceeding $\sqrt{n}$ and Conclude that n is prime if it is not divisible by any of these primes.

Example:

Show that 101 is prime

Sol:

$n = 101$

primes less than equal to $\sqrt{101}$ (i.e less than equal to 10):

2, 3, 5, 7

As,

$2 \nmid 101$ , $3 \nmid 101$ , $5 \nmid 101$ and $7 \nmid 101$

So, 101 is prime

---

Note: The above brute force is not efficient. It has exponential time Complexity.

Suppose we have

$n$ = 1000 digit number $\sim 10^{1000}$

we have to try approximately $\sqrt{n}$ different prime numbers to decide $n$ is prime or not i.e.,

$$\sqrt{n} = \sqrt{10^{1000}} = \left(10^{500 \times 2}\right)^{1/2} \approx 10^{500}$$

$n$ = 2 digit number
i.e $n$ = 0 to 99
$n = 10^2$

$n$ = 3 digit number
$n = 10^3$
So $n$ = 1000 digit
$n = 10^{1000}$

JUST FOR INFORMATION

Suppose we make a test for $\frac{10^{500}}{2}$ (half of the numbers)

i.e total # of division Checks/operation $\approx \frac{10^{500}}{2}$

Assume, we have a supper Computer (takes 1 sec for 5 billion operations)

$$= \frac{5 \text{ billion operations}}{1 \text{ Sec}} = 5 \times 10^9 \text{ operations in 1 sec.}$$

Total # of division tests $= \frac{10^{500}}{2}$

Time taken by total # of divisions $= \frac{10^{500}/2}{5 \times 10^9} \approx 10^{490}$ Seconds

$\approx 3 \times 10^{482}$ years

$\approx 2 \times 10^{472}$ ages of universe

---

## PRIME FACTORIZATION:

Because every integer has a prime factorization, it would be useful to have a procedure for finding this prime factorization.
This procedure is illustrated by the following example.

**Ex:** Find the prime factorization of 7007

1. Perform divisions of 7007 by succesive primes beginning with 2.

$2 \nmid 7007$ , $3 \nmid 7007$ , $5 \nmid 7007$ , $7 \mid 7007$

$7 \mid 7007$ i.e $\frac{7007}{7} = 1001$

So we can write it as

$$7007 = 7 \cdot 1001 \quad \text{——} \ (A)$$

2. Perform divisions of 1001 by succesive primes beginning with 7.

As $7 \mid 1001$ i.e $\frac{1001}{7} = 143$

So we can write it as

$1001 = 7 \cdot 143$ putting in (A), we have

$$7007 = 7 \cdot 7 \cdot 143 \quad \text{——} \ (B)$$

3. Perform divisions of 143 by successive primes beginning with 7.

$7 \nmid 143$ , $11 \mid 143$

$11 \mid 143$ i.e $\frac{143}{11} = 13$ , So

we can write it as

$143 = 11 \cdot 13$ putting in (B), we have

$$7007 = 7 \cdot 7 \cdot 143 = 7 \cdot 7 \cdot 11 \cdot 13 = 7^2 \cdot 11 \cdot 13$$ (Prime factors)

(STOP as for 13 , $11 \nmid 13$)

# THE SIEVE OF ERATOSTHENES

The Sieve of Eratosthenes is used to find all primes not exceeding a specified positive integer.

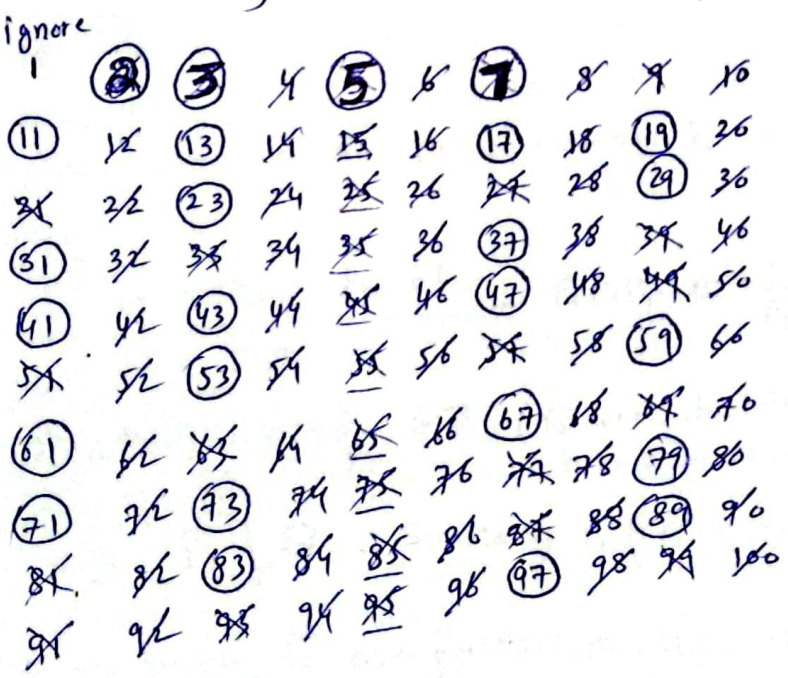
Example: Find all primes not exceeding 100

Procedure:

1. Make a list of 100 integers
2. The integers that a divisible by 2, other than 2, are deleted.
3. Because 3 is the next integer left after 2, all those integers divisible by 3, other than 3, are deleted.
4. Because 5 is the next integer left after 3, all those integers divisible by 5, other than 5, are deleted.
5. Because 7 is the next integer left after 5, all those integers divisible by 7, other than 7, are deleted.

Because all Composite integers not exceeding 100 are divisible by 2, 3, 5, 7 (i.e prime #s less than equal to $\sqrt{100}$). So we Stop the procedure.

AND, all remaining integers except 1 are primes.




Primes less than 100 are:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53
59, 61, 67, 71, 73, 79, 83, 89 and 97.

**THEOREM:**

There are infinitely many primes

**PROOF:**

We will prove this theorem using a proof by Contradiction.

Suppose, there are finitely many primes.

$$\text{i.e} \quad = \{P_1, P_2, P_3, \cdots, P_n\}$$

Let we take a number $Q$ bigger than all primes i.e this $Q$ is not prime i.e $Q$ is Composite number.

$$Q = P_1 \cdot P_2 \cdot P_3 \cdot \cdots P_n + 1$$

(bigger than all primes) and Composite number can be written as product of primes

Composite $Q$ means:

It has a prime divisor i.e Some prime number divides Composit.

i.e. $\frac{Q}{P_1}$ or $\frac{Q}{P_2}$ or $\cdots \frac{Q}{P_n}$ etc.

**Fundamental theorem of Arithmetic**

Every number either is prime or it can be written as product of primes.

Suppose we Consider prime number $P_1$ divides $Q$.

$$= \frac{P_1 P_2 P_3 \cdots P_n + 1}{P_1} = P_2 P_3 P_4 \cdots P_n + \frac{1}{P_1}$$

$$= P_2 P_3 \cdots P_n + \frac{1}{P_1} \notin \mathbb{Z} \quad (Q \text{ when divide by } P_1 \text{ has remainder})$$

$$\Rightarrow P_1 \nmid Q \text{, Similarly } P_2 \nmid Q, P_3 \nmid Q \text{ etc}$$

i.e no prime $P_i$ are factors as they all have remainders.

we found Contradiction here, we have assumed $Q$ is Composite but we found $Q$ is prime ($Q$ is not composite).

As $Q$ is larger than our set of finit primes and $Q$ is also prime other than $P_1, P_2, P_3 \cdots P_n$. So we Conclude There are infinitely many primes. Our assumption was wrong.

# MERSENNE PRIMES

Because there are infinitely many primes, given any positive integer there are primes greater than this number. There is an ongoing quest to DISCOVER LARGER AND LARGER PRIME NUMBER. The largest prime known has been an integer of the special form $2^p - 1$, where p is also prime. Such primes are called MERSENNE PRIMES.

MERSENNE PRIME:

$$M_p = 2^p - 1$$

: if you have a larger prime p, then using this form, you can find another extremely large prime (exponentially large prime)

$M_2 = 2^2 - 1 = 3$ (prime)
$M_3 = 2^3 - 1 = 7$ (prime)
$M_5 = 2^5 - 1 = 31$ (prime)
≡ ≡ ≡
$M_{11} = 2^{11} - 1 = 2047$ (not a prime)

: Mersenne number associated to that prime may or may not be prime It will be a Candidate of prime. Further, tests is required to figure it out.

NOTE:
$2^n - 1$ cannot be prime when n is not prime. But if n is prime, then it may be prime or it may not prime.

- The reason that the largest known prime has usually been Mersenne prime is that
  There is extremely efficient test known as LUCAS-LEHMER test, for determining whether $2^p - 1$ is prime. (would take exponential time)
- It is not currently possible to test numbers not of this Mersenne form.
- The last seven largest primes that humanity discovered, everyone used Mersenne numbers (The numbers have the form $2^n - 1$).

GIMPS: Great Internet Mersenne Prime Search

This software is used to help humanity to discover larger Prime numbers. You can join this search and possibly even WIN A CASH PRIZE.

LARGEST DISCOVERED PRIME NUMBER (till 2018)

$$M_{82,589,933} = 2^{82,589,933} - 1$$ = Number with 24 Million decimal Places.

# CONJECTURES AND OPEN PROBLEMS ABOUT PRIMES

It is easy to formulate Conjectures in Number Theory. Some conjectures are difficult to prove and others that remained open problems for many years. We describe some Conjectures here in number Theory.

1. Conjecture for Polynomial function:

Consider the polynomial $f(n) = n^2 - n + 41$ which results in prime numbers for $n \leq 40$.

For Example: $f(1) = 41$, $f(2) = 43$, $f(3) = 47$, $f(4) = 53$ and so on.

This can Lead us to the Conjecture that

> $f(n)$ is prime for all positive integers $n$

If we had such a polynomial function, we could find large primes for use in cryptography and other applications.

Can we settle this Conjecture?

> Looking for such a function, we might check out different polynomial functions, as some mathematicians did several hundred years ago.

Solution:

As $f(n) = n^2 - n + 41$ is prime for $n \leq 40$, but is composite for $n = 41$ as

$$f(41) = (41)^2 - 41 + 41 = (41)^2$$

We might be tempted to find a different polynomial for which $f(n)$ is prime for all positive integers $n$.

However, there is no such polynomial

**NOTE:**

It Canbe shown that

For every polynomial $f(n)$ with integer Coefficients, there is a positive integer $Y$ such that

$f(Y)$ is Composite

## 2. GOLDBACH'S CONJECTURE

Many famous problems about primes still await ultimate resolution by clever people, and better known as open problems, e.g., Goldbach's Conjecture.

Goldbach's Conjecture:

Every even integer $n$, $n > 2$, is the sum of two primes.
For example:

$4 = 2+2$, $6 = 3+3$, $8 = 3+5$, $10 = 5+5$ $(3+7)$ $12 = 7+5$ and so on.

As of early 2018, Goldbach's Conjecture has been checked for all positive even integers upto $4 \cdot 10^{18}$.

Although no proof of Goldbach' Conjecture has been found, most mathematicians believe it is true.

Some Conjectures similar to Goldbach's Conjecture have been proved, but they establishing results weaker than Goldbach's Conjecture. They are:

a. Every even integer $n > 2$, is the sum of at most six primes (proved 1995)

b. Every sufficiently large +ve integer is the sum of prime and a number that is either prime or product of two primes (proved 1966).

## 3. Infinitely Many Primes of the form $n^2+1$.

There are infinitely many primes of the form $n^2+1$, where $n$ is a positive integer. (open problem)

For Example:

$2^2+1 = 5$, $4^2+1 = 17$, $6^2+1 = 37$ and so on.

The best result currently known is that

There are infinitely many positive integers $n$ such that

$n^2+1$ is prime or product of atmost two primes (proved 1973).

## 4. THE TWIN PRIME CONJECTURE:

TWIN PRIMES are pairs of primes that differ by 2, such as

3 and 5, 5 and 7, 11 and 13, 17 and 19 etc.

The twin prime Conjecture asserts that

"There are infinitely many twin primes."

The strongest result proved Concerning twin primes is that there are infinitely many pairs p and p+2, where p is prime and p+2 is prime or product of two primes (proved 1966).

The world's record for twin primes ~~, as of early 2018, Consist of the numbers~~

As of August 2022, the Current Largest twin prime pair Known is:

$$2996863034895 \times 2^{1290000} \pm 1$$

with 388342 decimal digits. (It was discovered in 2016).

# 4.3/(B) GREATEST COMMON DIVISOR

The largest integer that divides both of the two integers is called the greatest common divisor of these integers.

**DEFINITION:**

Let $a$ and $b$ be integers, not both zero. The largest integer $d$ such that $d|a$ and $d|b$ is called the greatest common divisor of $a$ and $b$.

**ONE WAY TO FIND GCD:**

- Find all the positive common divisors of both integers
- Take the largest divisor

**Example:**

What is the greatest common divisor of 24 and 36.

**Sol:**

Positive divisors of 24 = 1, 2, 3, 4, 6, 12

Positive divisors of 36 = 1, 2, 3, 4, 6, 9, 12, 18

Common Divisors = 1, 2, 3, 4, 6, (12)

Greatest Common Divisor = 12

$$\gcd(24,36) = 12$$

**SECOND WAY: (By USING Prime Factorization)**

Prime factors of $a$ $\quad a = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdots p_n^{a_n}$

Prime factors of $b$ $\quad b = p_1^{b_1} \, p_2^{b_2} \, p_3^{b_3} \cdots p_n^{b_n}$

$$\gcd(a,b) = p_1^{\min(a_1,b_1)} \cdot p_2^{\min(a_2,b_2)} \cdots p_n^{\min(a_n,b_n)}$$

**Example:**

What is the greatest common divisor of 120 and 500.

**Sol:**

Prime factors of $120 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 = 2^3 \cdot 3^1 \cdot 5^1$

Prime factors of $500 = 2 \cdot 2 \cdot 5 \cdot 5 \cdot 5 = 2^2 \cdot 5^3$

| 2 \| 500 |
|---|
| 2 \| 250 |
| 5 \| 125 |
| 5 \| 25 |
| \| 5 |

| 2 \| 120 |
|---|
| 2 \| 60 |
| 2 \| 30 |
| 3 \| 15 |
| \| 5 |

$$\gcd(120,500) = 2^{\min(3,2)} \cdot 3^{\min(1,0)} \cdot 5^{\min(1,3)}$$

$$= 2^2 \cdot 3^0 \cdot 5^1 = 4 \cdot 1 \cdot 5 = 20$$

## Relative Prime:

The integers a and b are relative primes if their greatest common divisor is 1.

Example:

Are the integers 17 and 22 relative primes?

Sol:

Divisors of 17 = 1, 17
Divisors of 22 = 1, 2, 11
Common Divisors = 1 (no common other than 1)

$\gcd(17, 22) = 1$

So, 17 and 22 are relative primes.

## Pairwise Relatively Primes:

The integers $a_1, a_2, \dots a_n$ are pairwise relatively primes if

$$\gcd(a_i, a_j) = 1, \text{ whenever } 1 \le i < j \le n$$

Example:

Determine whether the following are pairwise relatively Primes.

- 10, 17, 21
- 10, 19, 24

Sol:-

- 10, 17, 21

  $\gcd(10,17) = 1$, $\gcd(10,21) = 1$ and $\gcd(17,21) = 1$

  So, 10, 17, 21 are relatively Primes.

- 10, 19, 24

  $\gcd(10,19) = 1$, $\gcd(19,24) = 1$, $\gcd(10,24) = 2$ (not equal to 1)

  So, 10, 19, 24 are not relatively Primes.

## LEAST COMMON MULTIPLES

$$LCM(a,b) = P_1^{\max(a_1,b_1)} \cdot P_2^{\max(a_2,b_2)} \cdot P_3^{\max(a_3,b_3)} \cdots P_n^{\max(a_n,b_n)}$$

Example:

What is the Least Common Multiples of

Prime Factors of $a = 2^3 \cdot 3^5 \cdot 7^2$
Prime Factors of $b = 2^4 \cdot 3^3$

$$LCM(a,b) = 2^{\max(3,4)} \cdot 3^{\max(5,3)} \cdot 7^{\max(2,0)} = 2^4 \cdot 3^5 \cdot 7^2 =$$

## Relationship Between GCD and LCM:

Let a and b be integers, then $ab = \gcd(a,b) \cdot lcm(a,b)$

# THE EUCLIDEAN ALGORITHM

Computing the greatest common divisor of two integers directly from prime factorization of these integer is INEFFECIENT.

**Reason :** Time Consuming to Find Prime Factorizations

THE EUCLIDEAN ALGORITHM is more efficient method of finding the greatest Common Divisor.

The Euclidean Algorithm is based on the following result about Greatest Common Divisors and the Division Algorithm :

**LEMMA :**

Let $a = bq + r$ , where $a, b \in \mathbb{Z}$

$q$ (quotient), $r$ (remainder) $\in \mathbb{Z}$

then

$$\gcd(a, b) = \gcd(b, r)$$

Proof :

Let $a = bq + r$

we suppose , d is a common divisor of a and b.

$d \mid a$ and $d \mid b$

As $d \mid b$ , then $d \mid bq$ (By Division Algorithm: $a \mid b$, then $a \mid bc$)

Also $d \mid a - bq$ : By $d \mid a$ , $d \mid bq$ then $d \mid a - bq$

$\Rightarrow d \mid r$ ( $a = bq + r$ or $a - bq = r$)

Now we have

$d \mid b$ and $d \mid r$ : d is a Common divisor of b and r

So, Any Common divisor of a and b is also a Common divisor of b and r.

**NOTE :**

If we can show that Common divisors of $(a, b)$ are the same as the Common divisors of $(b, r)$.

We will have shown that

$$\gcd(a, b) = \gcd(b, r)$$

because both pairs must have the same greatest Common divisor.

THE EU

Let $a = bq + r$

Now we suppose d is a common divisor of b and r.

$d|b$ and $d|r$

As $d|b$, then according to divison algorithm $d|bq$ for some q.

As $d|r$ and $d|bq$, then division algorithm says $d|bq+r$

Now have

$d|bq+r$ or $d|a$ (as $a = bq+r$)

As we Know

$d|a$ and $d|b$

So, Any common divisor of b and r is also a common divisor of a and b.

we have shown that
any common divisor of a, b is also a common divisor of b, r and
any common divisor of b, r is also a common divisor of a, b
So, we can say that
Both pairs must have the same greatest common divisor

$$\gcd(a,b) = \gcd(b,r) \quad \text{(Proved)}$$

## THE EUCLIDEAN ALGORITHM

As we Know

$$\gcd(a,b) = \gcd(b,r)$$ (reduced form)

where $\gcd(a,b)$: a, b are integer

$\gcd(b,r)$: b, smallest of the a and b
r, remainder

We use succesive divisions to reduce the problem of finding the GCD of two positive integers to the same problem with smaller integers, until one of the integers is zero.

Suppose that $a, b \in \mathbb{Z}$ with $a \geq b$ and Let $r_0 = a$, $r_1 = b$.
Successively apply division algorithm:

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

Because, the sequence of remainders $a = r_0 > r_1 > r_2 \cdots \geq 0$ cannot contain more than a terms, a remainder of zero occurs in this sequence of successive divisions.
Further more, it follows from Lemma that

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

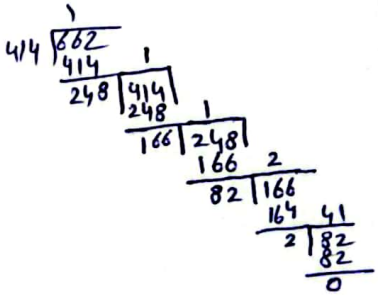
Hence, the greatest common divisor is the last nonzero remainder in the sequence of divisions.

**Example:**

Find the greatest common divisor of 414 and 662 using Euclidean Algo.

**Sol:**

$$662 = 414 \cdot 1 + 248$$
$$414 = 248 \cdot 1 + 166$$
$$248 = 166 \cdot 1 + 82$$
$$166 = 82 \cdot 2 + 2$$
$$82 = 2 \cdot 41 + 0 \qquad \gcd(414, 662) = 2$$




We can summarize these steps in tabular form:

| j | $r_j$ | $r_{j+1}$ | $q_{j+1}$ | $r_{j+2}$ |
|---|---|---|---|---|
| 0 | 662 | 414 | 1 | 248 |
| 1 | 414 | 248 | 1 | 166 |
| 2 | 248 | 166 | 1 | 82 |
| 3 | 166 | 82 | 2 | 2 |
| 4 | 82 | 2 | 41 | 0 |

**Algorithm:**

```
Procedure gcd (a, b : +ve int)
    x := a
    y := b
    While y ≠ 0
        r := x mod y
        x := y
        y := r
    return x {gcd of a, b}
```

**Time Complexity:**
# of divisions required to find gcd of a and b where $a \geq b$ is

$O(\log b)$

# GCD AS LINEAR COMBINATIONS:

## BÉZOUT'S THEOREM:

If a and b are positive integers, then there exist integers s and t (called Bézout Coefficients), such that

$$\gcd(a,b) = sa + tb \quad \text{:(called Bézout Identity)}$$

i.e., gcd(a,b) can be expressed as linear combination with integer coefficients of a and b.

Example:
As gcd(6,14) = 2 and
gcd(a,b) = sa + tb
gcd(6,14) = s·6 + t·14
2 = (-2)·6 + 1·14

There are two methods to find linear combination of the two integers equal to their GCD.

- using forward, backward pass
- using Extended Euclidean Algorithm

Example:

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

Sol:

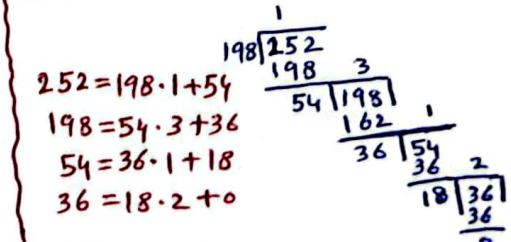
This method requires forward pass and a backward pass through the steps of the Euclidean algorithm.

We summarize the steps in tabular form:

| j | $r_j$ | $r_{j+1}$ | $q_{j+1}$ | $r_{j+2}$ |
|---|---|---|---|---|
| 0 | 252 | 198 | 1 | 54 |
| 1 | 198 | 54 | 3 | 36 |
| 2 | 54 | 36 | 1 | 18 |
| 3 | 36 | 18 | 2 | 0 |

Euclidean Algorithm uses the divisions to find gcd(252,198) as:

252 = 198·1 + 54
198 = 54·3 + 36
54 = 36·1 + 18
36 = 18·2 + 0




using the next-to-last division:

18 = 54 − 1·36 :(As 54 = 1·36 + 18)
18 = 54 − 1·(198 − 3·54) :(As 198 = 54·3 + 36)
= 54 − 1·198 + 3·54
= 4·54 − 1·198
= 4·(252 − 1·198) − 1·198 :(As 252 = 1·198 + 54)
= 4·252 − 4·198 − 1·198
18 = 4·252 − 5·198 required form

gcd(a,b) = sa + tb
s = 4
t = −5

$r_0 = r_1 q_1 + r_2$
$r_1 = r_2 q_2 + r_3$
=
$r_{n-2} = r_{n-1} q_{n-1} + r_n$
$r_{n-1} = r_n q_n + 0$

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

Example:

Express gcd(252, 198) as a linear Combination of 252, 198 using Extended Euclidean Algorithm.

Sol:

The main advantage of extended Euclidean algorithm is that it uses one pass through the steps of the Euclidean algorithm to find the Bezout Coefficients of a and b for its Linear Combination.

For Single pass we Set

$s_0 = 1 \quad t_0 = 0$
$s_1 = 0 \quad t_1 = 1$

and Let

$s_j = s_{j-2} - q_{j-1} s_{j-1}$ for $j = 2, 3, 4, \cdots, n$

$t_j = t_{j-2} - q_{j-1} t_{j-1}$ where $q_j$ are quotients in the division used when Euclid algorithm finds gcd(a,b).

We Summarize the steps of the extended Euclidean algorithm

| j | $r_j$ | $r_{j+1}$ | $q_{j+1}$ | $r_{j+2}$ | $s_j$ | $t_j$ | |
|---|---|---|---|---|---|---|---|
| 0 | 252 | 198 | 1 | 54 | 1 | 0 | $s_0=1, t_0=0$ |
| 1 | 198 | 54 | 3 | 36 | 0 | 1 | $s_1=0, t_1=1$ |
| 2 | 54 | 36 | 1 | 18 | 1 | -1 | $(s_2 = s_0 - q_1 s_1 = 1-1\cdot 0 = 1$ & $t_2 = t_0 - q_1 t_1 = 0-1\cdot 1 = -1)$ |
| 3 | 36 | 18 | 2 | 0 | -3 | 4 | $(s_3 = s_1 - q_2 s_2 = 0-3\cdot 1 = -3$ & $t_3 = t_1 - q_2 t_2 = 1-3\cdot(-1) = 1+3 = 4)$ |
| 4 | | | | | 4 | -5 | $(s_4 = s_2 - q_3 s_3 = 1-1\cdot(-3) = 4$ & $t_4 = t_2 - q_3 t_3 = -1-1\cdot 4 = -5)$ |

Here we have final

$s_4 = 4, \quad t_4 = -5$ : these are Bezout's Coefficients

So, we can write as :

$$\gcd(254, 198) = s \cdot 254 + t \cdot 198$$

$$18 = 4 \cdot 254 + -5 \cdot 198$$

18, the greater Common divisor of 252 and 198, Can be expressed as Linear Combination of 254 and 198 with Bezout Coefficients 4 & -5 as

$$18 = 4 \cdot 254 + (-5) \cdot 198$$

**LEMMA:**

If $a, b$ and $c$ are positive integers such that $\gcd(a,b)=1$ and $a \mid bc$, then $a \mid c$.

**Proof:**

Because we have $\gcd(a,b)=1$, then by Bezout's theorem there are integer $s$ and $t$ such that

$$sa+tb=1 \quad -\text{Ⓐ} \quad (\text{i.e. } 1 \text{ (} \gcd(a,b) \text{) can be expressed as } sa+tb)$$

Multiplying both sides of Ⓐ by $c$, we obtain

$$sac+tbc=c \quad -\text{Ⓑ}$$

as we have $a \mid bc$ (given), then according to fundamental theorem of arithmetic

$$a \mid bc \cdot t \quad -\text{①}$$

and clearly we have

$$a \mid sac \quad -\text{②} \quad (a \text{ is in numerator, so } a \text{ divides the term with a multiple})$$

From ① and ②, we have

$$a \mid bct+sac \qquad (\text{we know As if } a \mid b \text{ and } a \mid b, \text{ then } a \mid b+c)$$

or $a \mid c$ (we have eq Ⓑ, $sac+tbc=c$)

So we conclude that

if $\gcd(a,b)=1$ and $a \mid bc$, then

$$a \mid c \quad (\text{proved})$$

**THEOREM** : 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 nondecreasing size.

**Proof: Part 1**

Let $n$ be any integer greater than 1, then $n$ must have atleast one prime factor say $P_1$.

then there exist $n_1$ such that ①

$$n = P_1 n_1 \quad \text{, wher } n > n_1 \quad \text{: divisible algorithm}$$

If $n_1 = 1$, then $n = P_1$ : proved

If $n_1 > 1$, then $n_1$ must have at least one prime factor $P_2$.

and there exist $n_2$ such that ②

$$n_1 = P_2 n_2 \text{, where } n_1 > n_2$$

From ① and ②

$$n = P_1 n_1$$
$$n = P_1 P_2 n_2$$

Similarly, $n$ can be expressed as

$$n = P_1 P_2 P_3 \cdots P_K n_K$$

or $$n = P_1 P_2 P_3 \cdots P_K \cdot 1 \qquad n_K = \text{least natural number} = 1$$

$$n = P_1 P_2 P_3 \cdots P_K$$

Completed first part i.e.,

Every integer greater than 1 can be expressed as a prime or as the product of primes.

**Proof : Part 2** (Uniqueness of Prime factorization of a positive integer)

We use a proof by Contradiction.

Suppose that the positive integer n can be written as the product of primes in two different ways:

$$n = P_1 P_2 P_3 \cdots P_k$$
$$= q_1 q_2 q_3 \cdots q_r$$

So, We can write it as :

$$P_1 P_2 P_3 \cdots P_k = q_1 q_2 q_3 \cdots q_r$$ : factorization of the same number.

By divisibility, we know

$$P_1 \mid q_1 q_2 q_3 \cdots q_r$$ : $P \cdot n = 2$ $(3 \times 2 = 6)$, $P \mid 2$ $(3 \mid 6)$

i.e $P_1$ divides at least one of $q_1, q_2, q_3, \cdots q_r$

Suppose $P_1 \mid q_1$ and as $P_1$ & $q_1$ are both primes,

So $P_1 \mid q_1$ is only possible if $P_1 = 1$ or $P_1 = q_1$

As $P_1$ is prime, so it could not be possible that $P_1 = 1$, so

we can say that

$$P_1 = q_1$$

Similarly,

$P_2 \mid q_1, q_2, \cdots q_r$ or we assume that $P_2 \mid q_2$, so $P_2 = q_2$

and $P_3 \mid q_1, q_2, \cdots q_r$ or we assume that $P_3 \mid q_3$, so $P_3 = q_3$

$\equiv$

and so on.

So, we can say that

$$P_i = q_i \quad \text{for } i = 1, 2, \cdots k$$ (all $P_i$'s equal $q_i$'s)

Now we have to show that

$$r = k$$

To show $r = K$

We use Contradiction.

Suppose $r = K$ and let $K < r$.

So, we can write it as

$$P_1 P_2 P_3 \cdots P_K = q_1 q_2 q_3 \cdots q_K \cdots q_r$$

i.e., $$1 = q_{K+1} q_{K+2} \cdots q_r$$

$$1 = \text{product of } (r-K) \text{ primes}$$

Is it possible that product of primes equals 1 (as least prime is 2).

Answere is no.

So $r = K$

this Completes the uniqueness part.