G C D
(The Greatest Common Divisor)

21PC32 - SATHEESH KUMAR R S

The GCD of n Positive Numbers

The gcd of n numbers where (n>=2) positive numbers $a_1 , a_2, a_3 , . . . , an$ is the the largest positive integer that divides each ai where i in the range [1 , n] . It is denoted by

$$gcd (a_1 , a_2 , a_3 , ... , an) .$$

Example :

Find gcd (12 , 18 , 28) , gcd (12 , 36 , 60 , 108) and gcd (15 , 28 , 50) .

Solution :

i) The Largest Positive Integer that divides 12 , 18 and 28 is 2 .

So gcd (12 , 18 , 28) = 2 .

ii) The Largest Positive Integer that divides 12 , 36 , 60 , 108 is 12 .

The Common greatest factor of the above numbers is 12 .

So gcd (12 , 36 , 60 , 108) = 12 .

iii) The Largest Positive Integer that divides 15 , 28 , 50 is 1 .

The Common greatest factor of the above numbers is 1 .

So gcd (15 , 28 , 50) = 1 .

Example :

Using Recursion , Evaluate (18 , 30 , 60 , 75 , 132)

Solution :

In order to find gcd (a_1 , a_2 , a_3 , ... , an) we should find it for gcd (gcd (a_1 , a_2, . . an-1) , an) and for it gcd (gcd (gcd (a_1 , a_2 , . . . , an-2) , an-1) , an) and proceed till it makes to calculate for pair of numbers .

So by using the above statement ,

gcd (18 , 30 , 60 , 75 , 132) = gcd (gcd (18 , 30 , 60 , 75) , 132)

= gcd (gcd (gcd (18 , 30 , 60) , 75) , 132)

= gcd (gcd (gcd (gcd (18 , 30) , 60) , 75) , 132)

we know that gcd (18 , 30) = 6 .

Substitute it in the above and proceed the same procedure .

$= \gcd(\gcd(\gcd(6, 60), 75), 132)$ $\Longrightarrow \gcd(6, 60) = 6$

$= \gcd(\gcd(6, 75), 132)$ $\Longrightarrow \gcd(6, 75) = 3$

$= \gcd(3, 132)$ $\Longrightarrow \gcd(3, 132) = 3$

$= 3$

Therefore $\gcd(18, 30, 60, 75, 132) = 3$.

Corollary :

If the $\gcd(a_1, a_2, a_3, a_4, \ldots, an) = d$ then $d \mid ai$ for every integer i, where $1 \le i \le n$. i.e., d divides ai where i belongs to $[1, n]$.

Corollary :

If $a_1, a_2, a_3, \ldots, an$ be the numbers then there exists d such that $d \mid (a_1 * a_2 * a_3 * \ldots * an)$ and $\gcd(d, ai) = 1$ for $1 \le i \le n-1$ then $d \mid an$.

Example :

If the numbers be 7 , 5 , 3

then $7 * 5 * 3 = 105$

if $d = 3$ then $d \mid 105$ such that $\gcd(d, ai) = 1$ where $1 \leq i \leq n - 1$ so that $d \mid 3$ which is $d \mid an$ and also d can also take 1 for each case .

Here the value of $d = 1$ and $d = 3$.

From this we can say that if d be any number and d divides $a_1 * a_2 * a_3 * .. * an$ and $\gcd(d, ai) = 1$ for every $1 \leq i \leq n - 1$ then $d \mid an$.

Linear Combination of n Positive Integers :

A Linear Combination of n positive integers $a_1, a_2, a_3, \ldots, an$ is a sum of the form $\alpha * a_1 + \beta * a_2 + \gamma * a_3 + \ldots + An * an$ where $\alpha, \beta, \gamma, \ldots, An$ are integers .

For Example :

The Linear Combination of the Numbers 12 , 15 and 21 is ,

$2 * 12 + (-2) * 15 + 15 * (-5)$ so that is yields 3 which is the gcd (12 , 15 , 21) .

Example :

Express the gcd (12 , 15 , 21) as a linear combination of 12 , 15 , 21 .

Solution :

First we need to find the gcd (12 , 15 , 21) which is 3 . Then find the values of α , β and γ such that $\alpha * 12 + \beta * 15 + 21 * \gamma = 3$. By trial and error method we came to know $\alpha = -1$, $\beta = 1$ and $\gamma = 0$ so that

$(-1) * 12 + 1 * 15 + 0 * 23 = 3$ [we will study later in Euclidean Algorithm how to efficiently find the values for α , β and γ] .

Corollary

If $a \mid c$ and $b \mid c$ and $\gcd(a, b) = 1$, then $a*b \mid c$.

Proof :

From given if $a \mid c$ and $b \mid c$ means $c = n * a$ and $c = m * b$

For some n, m belongs to Z.

And also $\gcd(a, b) = 1$ means the linear combination of a, b is

$\alpha * a + \beta * b = 1$. For some α, β belongs to Z.

Then

$$\alpha * a * c + \beta * b * c = c$$

Sub $c = n * a$ and $c = m * b$ in the above Equation ,

$$\alpha * a * m * b + \beta * b * n * a = c$$

$$ab(\alpha * m + \beta * n) = c$$

Therfore from the above we can conclude that $a*b \mid c$ ($a*b$ divides c) , Pairwise Relatively Prime Integers :

The Positive integers $a_1, a_2, a_3, \dots, a_n$ are pairwise relatively prime if Every pair of integers is relatively prime ; that is , $(a_i, a_j) = 1$, whenever $i \neq j$.

Corollary :

If the positive integers $a_1, a_2, a_3, \dots, a_n$ are pairwise relatively prime , then the $\gcd(a_1, a_2, a_3, \dots, a_n) = 1$.

For Example :

Let the numbers be 4 , 27 , 35 as they are relatively prime (there is no any common divisors for the above three numbers) their gcd is 1 .

Note :

The Converse of the above Corollary is not true ; that is if the $\gcd(a_1, a_2, a_3, \ldots, a_n) = 1$ then the integers are relatively prime numbers .
The counter example for this is , Let the numbers be 6 , 15 and 49 and their $\gcd(6, 15, 49) = 1$ but they are not relatively prime because 6 and 15 have common Divisor which is 3 . So the converse of the above corollary is not true .

Corollary :

There are Infinitely Many Primes. And for this corollary , proof is not necessary .

Theorem :

Let the numbers be $a_1, a_2, a_3, \ldots, a_n$ be positive integers, where $n >= 3$. Then $gcd(a_1, a_2, a_3, \ldots, a_n) = gcd(gcd(a_1, a_2, a_3, \ldots, a_{(n-1)}), a_n)$.

Proof :

Let the $gcd(a_1, a_2, a_3, \ldots, a_n) = d$, $gcd(a_1, a_2, a_3, \ldots, a_{(n-1)}) = d'$ and let $d'' = gcd(d', a_n)$.

We need to show that $d = d''$; $d \mid d''$ and $d'' \mid d$.

Since $d = gcd(a_1, a_2, a_3, \ldots, a_n)$, $d \mid a_i$ for $1 \leq i \leq n-1$ and $d \mid d'$ which also holds

$d \mid gcd(d', a_n) = d \mid d''$. $d'' = m * d$ ==➔ for some m belongs to Z

We also need to show that $d \mid d''$.

Since $d'' = \gcd(d', an)$ which means $d'' \mid d'$ and $d'' \mid an$; $d'' \mid d'$ - holds for $1 \leq i \leq n-1$. Thus d'' must divide d too . Hence $d'' \mid d$.

Hence we got $d \mid d''$ and $d'' \mid d$. Therefore $d = d''$

Then $\gcd(a_1, a_2, a_3, \ldots, an) = \gcd(\gcd(a_1, a_2, a_3, \ldots, a(n-1)), an)$

Hence Showed .

Exercises :

i) Using Recursion , find gcd (14 , 18 , 21 , 36 , 48)

Solution :

= gcd (gcd (14 , 18 , 21 , 36) , 48)

= gcd (gcd (gcd (14 , 18 , 21) , 36) , 48)

= gcd (gcd (gcd (gcd (14 , 18) , 21) , 36) , 48) ==➔ gcd (14 , 18) = 2

= gcd (gcd (gcd (2 , 21) , 36) , 48) ==➔ gcd (2 , 21) = 1

= gcd (gcd (1 , 36) , 48) ==➔ gcd (1 , 36) = 1

= gcd (1 , 48) ==➔ gcd (1 , 48) = 1

= 1

ii) Disprove the Below Statement .

If $(a , b) = 1 = (b , c)$ then $(a , c) = 1$.

Solution :

In order to disprove the above statement we should provide a Encounter example of it .

Assume that the given statement is true for any integers .

Let us have the values for a , b and c as $a = 2$, $b = 3$ and $c = 8$ such that the $\gcd (2 , 3) = \gcd (3 , 8) = 1$ but

$\gcd (2 , 8) \neq 1$; as it yields a contradiction of our assumption .

So it is clearly known that when $\gcd (a , b) = \gcd (b , c) = 1$ it is not suppose to be that $\gcd (a , c)$ should 1 .

Express the gcd of each pair as a linear combination of the numbers .

i) 18 , 28

ii) 12 , 15 , 18

Solution :

The gcd (18 , 28) = 2

Then find the values for α , β such that

$$\alpha * 18 + \beta * 28 = 2$$

From Trial and error method one such values for α and A_2 is $\alpha = -3$, $\beta = 2$.

So the Linear combination of the number 18 , 28 is

$$(-3) * 18 + 2 * 28 = 2$$

The gcd (12 , 15 , 18) = 3 .

Then find the values of α , β and γ such that the equation

$$\alpha * 12 + \beta * 15 + A_3 * 18 = 3$$

By trial and error method one such values of α , β and γ is :

$\alpha = 3$, $\beta = -1$, $\gamma = -1$ such that the Linear Combination of the numbers 12 , 15 and 18 is

$$3 * 12 + (-1) * 15 + (-1) * 18 = 3 .$$