Euclid’s Algorithm

Finding the GCD (Greatest Common Divisor) of a number:

Definition:

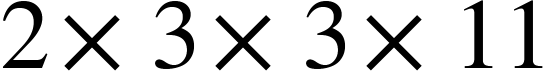
Let GCD(a,b)=g, then g is the greatest number where g|a and g|b.

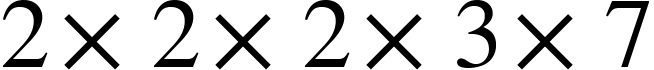
Here, g|a means g divides a.

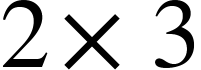
We can approach this in two ways:

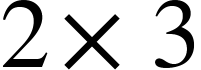
1.Finding all of the factors of both of the numbers and picking up the highest common factor in both the numbers

For example GCD of numbers (198,168)

Prime factors of 198: 

Prime factors of 168:

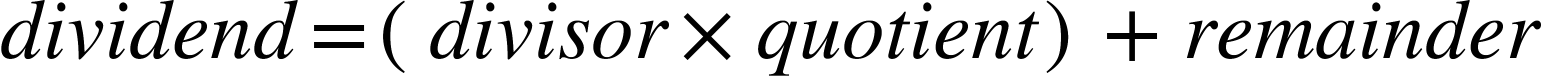
Common factors: 

GCD:  =6

2.Using Euclid’s Algorithm :

For the sake of understanding let’s just see what the algorithm says, we will come to the mathematical proof of it afterwards.

Algorithm Steps:

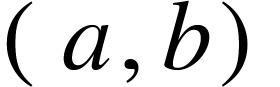
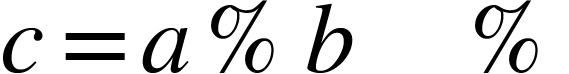
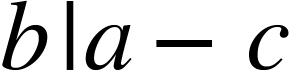
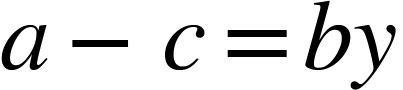
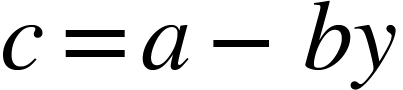
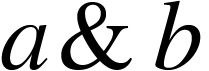
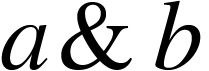
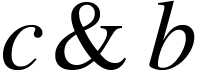
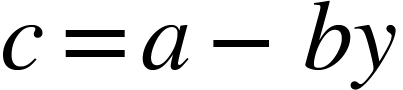
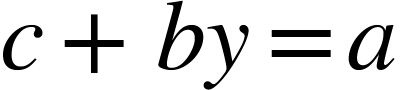
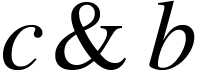
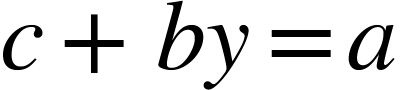
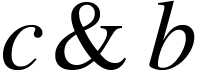
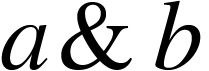
1. Take the greater of the two numbers as dividend and the other one as the divisor.
2. Perform the division of dividend and divisor.
3. 
4. Now, store back the remainder as the new divisor and the old divisor as the new dividend.

That is: new divisor⇐remainder

new dividend⇐ old divisor

1. Repeat from step 1 till divisor=0 and when divisor=0, the dividend is the GCD.

Mathematical Proof of the Euclid’s Algorithm

1. Let be the two numbers, whose GCD is to be calculated.
2. And <math xmlns="http://www.w3.org/1998/Math/MathML"><mi>c</mi></math> be the number where is the modulo operation.
3. This means that  (i.e b divides (a-c)).
4. Therefore,  ⇒ .
5. Let <math xmlns="http://www.w3.org/1998/Math/MathML"><mi>d</mi></math> be the number that divides 
6. Using step 4 and step 5, we can see that <math xmlns="http://www.w3.org/1998/Math/MathML"><mi>d</mi></math> divides <math xmlns="http://www.w3.org/1998/Math/MathML"><mi>c</mi></math> too.
7. Therefore, any common divisor of is also a common divisor of 
8. From step 4 we know that, ⇒.
9. So, any common divisor of  also divides <math xmlns="http://www.w3.org/1998/Math/MathML"><mi>a</mi></math> as 
10. Thus any common divisor of  is a common divisor of .
11. This is what we are doing in the algorithm.