Number Theory

This document covers

Definitions

Factors, Divisibility and modulo arithmetic

Fundamental Theorem of Arithmetic

HCF/LCM

Euclids Algorithm

Floor Ceiling Functions

## Facors, dividibility and Modulo arithmetic

## Definitions

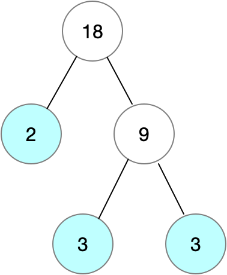
|  |  |
| --- | --- |
| Divisor | If we say p is a factor or divisor of q and q is divisible by p. P is a multiple of q |
| Fundamental theorum of Arithmetic | Any integer can be expressed as the product of prime factors |
| Highest Common Factor | The highest number that is a divisor of two number. Given two integers , and we can calculate the highest common factor as |
| Lowest Common Multiple | The lowest number which is a multiple of two numbers |
| Relating HCM and LCM |  |
| Euclids Algorithm |  |
| Floor |  |
| Ceiling |  |

## Fundamental Theorem of Arithmetic

Any integer is either prime itself prime or can be expressed as a product of prime factors

Where are successive primes and are powers of that prime. For any given p, the corresponding can be zero. We can find the prime factors of any given number by continually dividing through. The following shows how to extract the prime factors of 18

Figure 1 Prime Factorisation of 18

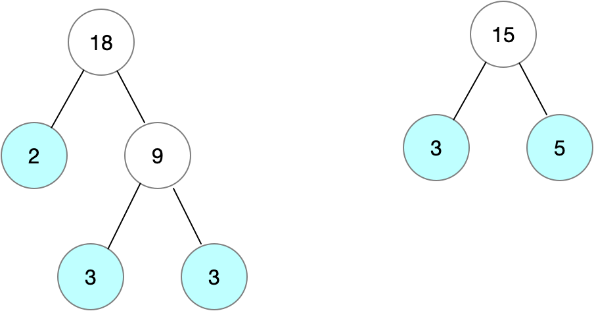


## HCF/LCM

### Highest Common Factor (HCF)

Given two integers x and y and their corresponding prime factorisations

We can calculate the highest common factor as

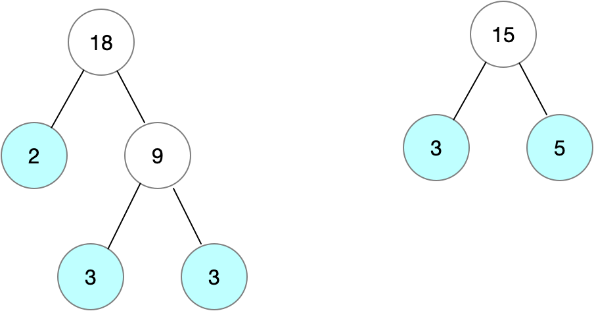


,

### Lowest Common Multiple (LCM)

Given two integers x and y and their corresponding prime factorisations

We can calculate the lowest common multiple as



### Relating HCF and LCM

Given two integers x and y and their corresponding prime factorisations

We can show there is a relationship between lcm and hcf.

So we now know that

This is very powerful as we have efficient algorithms for calculating the hcf, whereas we do not have efficient algorithms for carrying out prime factorisation.

## Euclids Algorithm for Gcd

#### Proof

##### Show that gcd(a,b) is a divisor of a-b

By the definition of a divisor we know that

##### Show that gcd(a,b) is a common divisor of b and a-b

In the previous step we showed that gcd(a,b) is a divisor of a-b and by definition gcd(a,b) is a divisor of b. We hence know that gcd(a,b) is a common divisor of a and a-b. We know that gcd(a,b) must be less than or equal to gcd(b,a-b) by the definition of gcd(b,a-b) as the **greatest** common divisor

##### Show that gcd(b,a-b) is a divisor of a

By the definition of a divisor we know that

##### Show that gcd(b,a-b) is a common divisor of a and b

By definition gcd(b,a-b) is a divisor of b and we have shown that gcd(b,a-b) is a divisor of a. So we know that gcd(b,a-b) is a common divisor of a and b. Because gcd(a,b) is the **greatest** common divisor of a and bwe know that

Taken (4) and (9) together we have shown that

##### Show that gcd(b,a-b)=gcd(b,a%b)

**We have shown that** . We can apply the formula multiple times

The definition of the % operator is

Letting and substituting into the right hand side of (10) we have

We have now proved Euclids algorithm that

#### Implementation (C#)



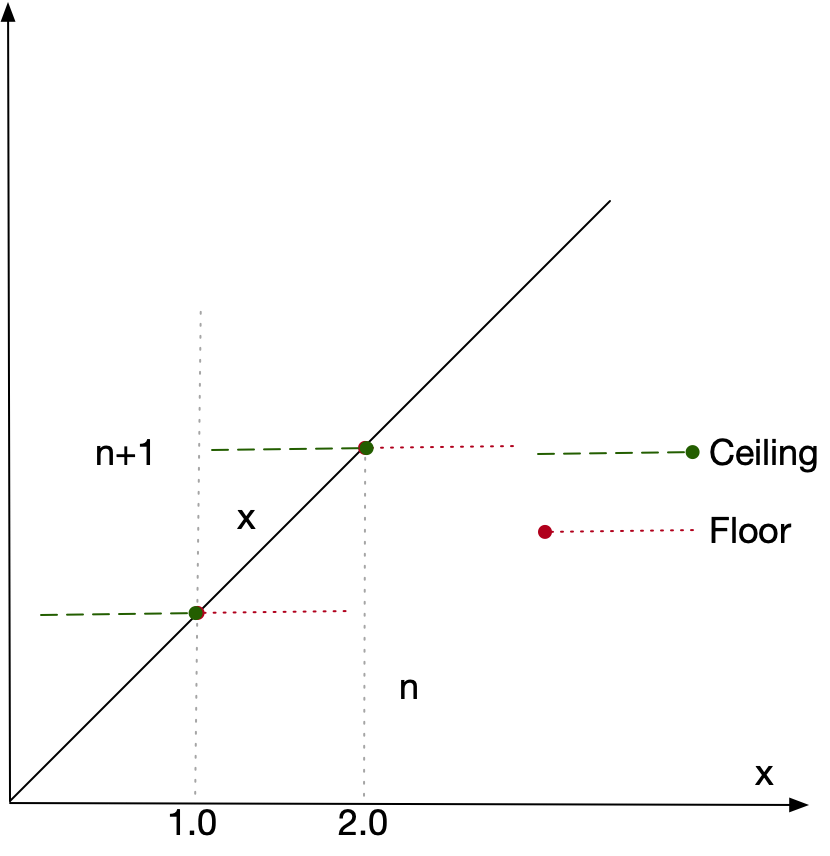
## Floor/Ceiling Functions

### Definitions

Floor – The greatest integer less than x

Ceiling – The smallest integer less than x

Figure 2Floor/Ceiling



Listing 1 Examples



Fractional Part

The floor gives the integer part of a real and subtracting the floor from the real gives the fractional part

We can use this notation to calculate possible values of

### Property Summary

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  | , if n is an integer and x a real |
|  | if n is an integer and x a real |
|  | , if n is an integer and x a real |
|  | if n is an integer and x a real |
|  | if f is continuous, monotonically increasing with the property that if then |

### Property Detail

#### Property 7

#### 

#### Property 8

#### 

#### Property 16

If we define function

where is **continuous** and **monotonically increasing** and where has the following special property

**Property P:** if then

Then for all for which the property P holds

#### Proof

In the simple case where we have nothing to do. We hence focus on the case where .

From the definition of the ceiling function

Because is monotonically increasing

Because ceiling is non decreasing

Assume

*Because ceiling only deals in integers*

This means the monotonically increasing function f must increase above in order to make it possible for This means that the following two things must be true

The special property P means that y must be an integer as is by definition an integer. But there cannot be an integer between x and so we have a contradiction and hence it is not possible for

and hence