

Number Theory

Definitions

Divisor

If $p|q$ we say p is a factor or divisor of q and q is divisible by p . P is a multiple of q

Fundamental theorem of Arithmetic

Any integer can be expressed as the product of prime factors $x = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$

Highest Common Factor

The highest number that is a divisor of two number.

Given two integers $x = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$, and $y = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$ we can calculate the highest common factor as $hcm(x, y) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \dots p_n^{\min(a_n, b_n)}$

Lowest Common Multiple

The lowest number which is a multiple of two numbers

Relating HCM and LCM

$$lcm(x, y) = \frac{x \times y}{hcf(x, y)}$$

Euclids Algorithm

$$gcd(a, b) = gcd(b, a \% b) \#(10)$$

Floor

$$floor : \mathcal{R} \rightarrow \mathbb{Z}$$

$$floor(x) = \lfloor x \rfloor = \max\{a \in \mathbb{Z} \mid a \leq x\}$$

Ceiling

$$ceiling : \mathcal{R} \rightarrow \mathbb{Z}$$

$$ceiling(x) = \lceil x \rceil = \max\{a \in \mathbb{Z} \mid a \leq x\}$$

Fundamental Theorem of Arithmetic

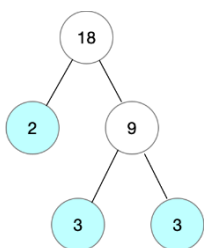
Any integer is either prime itself or can be expressed as a product of prime factors

$$x = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$$

Where $p_1 \dots p_n$ are successive primes and $a_1 \dots a_n$ are powers of that prime. For any given p , the corresponding a 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

$$18 = 2^1 \times 3^2$$

Figure 1 Prime Factorisation of 18



HCF/LCM

Highest Common Factor (HCF)

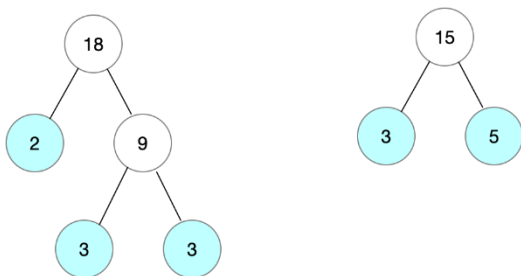
Given two integers x and y and their corresponding prime factorisations

$$x = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$$

$$y = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$$

We can calculate the highest common factor as

$$hcm(x, y) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \dots p_n^{\min(a_n, b_n)}$$



$$18 = 2^1 \times 3^2, 15 = 2^0 \times 3^1 \times 5^1$$

$$hcf(15,18) = 2^{\min(0,1)} \times 3^{\min(1,2)} \times 5^{\min(0,1)} = 3$$

Lowest Common Multiple (LCM)

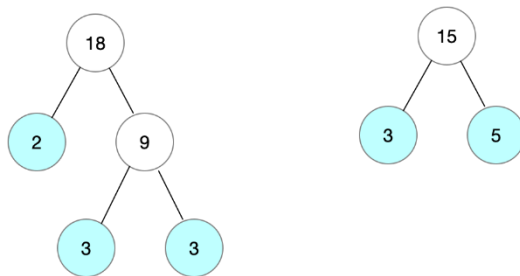
Given two integers x and y and their corresponding prime factorisations

$$x = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$$

$$y = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$$

We can calculate the lowest common multiple as

$$lcm(x, y) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \dots p_n^{\max(a_n, b_n)}$$



$$18 = 2^1 \times 3^2$$

$$15 = 2^0 \times 3^1 \times 5^1$$

$$lcm(15,18) = 2^{\max(0,1)} \times 3^{\max(1,2)} \times 5^{\max(0,1)} = 2 \times 3^2 \times 5^1 = 90$$

Relating HCF and LCM

Given two integers x and y and their corresponding prime factorisations

$$x = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$$

$$y = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$$

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

$$lcm(x, y) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \dots p_n^{\max(a_n, b_n)}$$

$$hcf(x, y) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \dots p_n^{\min(a_n, b_n)}$$

$$hcf(x, y) \times lcm(x, y) = p_1^{\min(a_1, b_1) + \max(a_1, b_1)} p_2^{\min(a_2, b_2) + \max(a_2, b_2)} \dots p_n^{\min(a_n, b_n) + \max(a_n, b_n)}$$

$$hcf(x, y) \times lcm(x, y) = p_1^{a_1 \times b_1} p_2^{a_2 \times b_2} \dots p_n^{a_n \times b_n} = x \times y$$

So we now know that

$$lcm(x, y) = \frac{x \times y}{hcf(x, y)}$$

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

$$a = x \times \gcd(a, b) \quad (1)$$

$$b = y \times \gcd(a, b) \quad (2)$$

$$a - b = (x - y) \times \gcd(a, b) \quad (3)$$

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

$$\gcd(a, b) \leq \gcd(b, a - b) \quad (4)$$

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

By the definition of a divisor we know that

$$a - b = m \times \gcd(b, a - b) \quad (5)$$

$$b = n \times \gcd(b, a - b) \quad (6)$$

$$a = (m + n) \times \gcd(b, a - b) \quad (8)$$

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 b we know that

$$\gcd(a, b) \geq \gcd(b, a - b) \quad (9)$$

Taken (4) and (9) together we have shown that $\gcd(a, b) = \gcd(b, a - b)$

Show that $\gcd(b, a-b) = \gcd(b, a \% b)$

We have shown that $\gcd(a, b) = \gcd(b, a - b) = \gcd(a - b, b)$. We can apply the formula multiple times

$$\gcd(a, b) = \gcd(a - b, b) = \gcd(a - 2b, b) = \gcd(a - qb, b) \quad (10)$$

The definition of the % operator is

$$a \% b = a - \left(\frac{a}{b}\right) \times b \quad (11)$$

Letting $q = \frac{a}{b}$ and substituting into the right hand side of (10) we have

$$\gcd(a, b) = \gcd(a - b, b) = \gcd(a - 2b, b) = \gcd(a \% b, b) = \gcd(b, a \% b) \quad (10)$$

We have now proved Euclids algorithm that

$$\gcd(a, b) = \gcd(b, a \% b) \quad (10)$$

IMPLEMENTATION (C#)

```
/// <summary>
/// Implementation of Euclids algorithm
/// </summary>
/// <param name="a"></param>
/// <param name="b"></param>
/// <returns></returns>
public static int HighestCommonFactor(int a, int b)
{
    if (a < b)
    {
        return HighestCommonFactor(b, a);
    }
    else
    {
        int remainder = a % b;

        if (remainder == 0)
        {
            return b;
        }
        else
        {
            return HighestCommonFactor(b, remainder);
        }
    }
}
```

Floor/Ceiling Functions

Definitions

Floor – The greatest integer less than x

$$\text{floor} : \mathcal{R} \rightarrow \mathbb{Z}$$

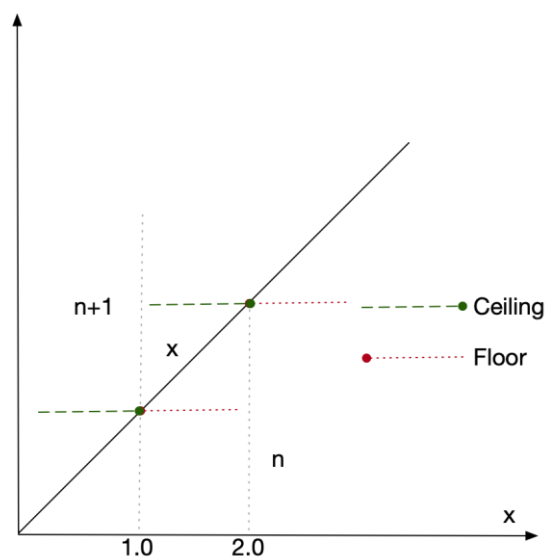
$$\text{floor}(x) = \lfloor x \rfloor = \max\{a \in \mathbb{Z} \mid a \leq x\}$$

Ceiling – The smallest integer less than x

$$\text{ceiling} : \mathcal{R} \rightarrow \mathbb{Z}$$

$$\text{ceiling}(x) = \lceil x \rceil = \max\{a \in \mathbb{Z} \mid a \leq x\}$$

FIGURE 2 FLOOR/CEILING



LISTING 1 EXAMPLES

- ♦ $\lfloor 1.0 \rfloor = \lceil 1.0 \rceil = 1$
- ♦ $\lfloor 1.0000001 \rfloor = 1$
- ♦ $\lceil 1.0000001 \rceil = 2$
- ♦ $\lfloor 1.9999999 \rfloor = 1$
- ♦ $\lceil 1.9999999 \rceil = 2$

Fractional Part

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

$$\{x\} = x - \lfloor x \rfloor$$

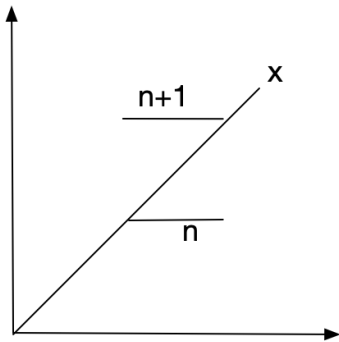
We can use this notation to calculate possible values of $\lfloor x + y \rfloor$

Property Summary

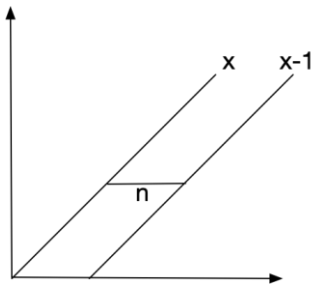
1. $\lfloor x \rfloor = \lceil x \rceil = x \leftrightarrow x \in \mathbb{Z}$
2. $x - 1 < \lfloor x \rfloor \leq \lceil x \rceil < x + 1, \quad x \in \mathbb{R}$
3. $\lfloor -x \rfloor = -\lceil x \rceil, \quad x \in \mathbb{R}$
4. $-\lfloor x \rfloor = \lceil -x \rceil, \quad x \in \mathbb{R}$
5. $\lfloor x \rfloor - \lceil x \rceil = 0 \leftrightarrow x \in \mathbb{Z}$
6. $\lfloor x \rfloor - \lceil x \rceil = 1 \leftrightarrow x \notin \mathbb{Z}$
7. $\lfloor x \rfloor = n \leftrightarrow n \leq x < n + 1, x \notin \mathbb{R}, n \notin \mathbb{Z}$
8. $\lceil x \rceil = n \leftrightarrow n - 1 < x \leq n, x \notin \mathbb{R}, n \notin \mathbb{Z}$
9. $\lfloor x \rfloor = n \leftrightarrow x - 1 < n \leq x, x \notin \mathbb{R}, n \notin \mathbb{Z}$
10. $\lceil x \rceil = n \leftrightarrow x \leq n < x + 1, x \notin \mathbb{R}, n \notin \mathbb{Z}$
11. $\left\lfloor \frac{x}{2} \right\rfloor + \left\lceil \frac{x}{2} \right\rceil = x$
12. $\lfloor x + n \rfloor = \lfloor x \rfloor + n$, if n is an integer and x a real
13. $\lceil x + n \rceil = \lceil x \rceil + n$, if n is an integer and x a real
14. $x < n \rightarrow \lfloor x \rfloor < n$, if n is an integer and x a real
15. $n < x \rightarrow n < \lceil x \rceil$ if n is an integer and x a real
16. $\lfloor f(\lfloor x \rfloor) \rfloor = \lfloor f(x) \rfloor$ if f is continuous, monotonically increasing with the property that if $f(x) \in \mathbb{Z}$ then $x \in \mathbb{Z}$

Property Detail

PROPERTY 7 $\lfloor x \rfloor = n \leftrightarrow n \leq x < n + 1, x \notin \mathbb{R}, n \notin \mathbb{Z}$



PROPERTY 8 $\lceil x \rceil = n \leftrightarrow n - 1 < x \leq n, x \notin \mathbb{R}, n \notin \mathbb{Z}$



PROPERTY 16

If we define function

$$f: \mathbb{R}' \rightarrow \mathbb{R} \mid \mathbb{R}' \subseteq \mathbb{R} \text{ is the domain of } f$$

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

Property P: if $f(x) \in \mathbb{Z}$ then $x \in \mathbb{Z}$

Then for all $x \in \mathbb{R}'$ for which the property P holds

$$\lceil f(\lceil x \rceil) \rceil = \lceil f(x) \rceil$$

PROOF

In the simple case where $x = \lceil x \rceil$ we have nothing to do. We hence focus on the case where $x \neq \lceil x \rceil$.

$$x \neq \lceil x \rceil \rightarrow x \leq \lceil x \rceil$$

From the definition of the ceiling function

$$x \leq \lceil x \rceil \rightarrow f(x) \leq f(\lceil x \rceil)$$

Because f is monotonically increasing

$$f(x) \leq f(\lceil x \rceil) \rightarrow \lceil f(x) \rceil \leq \lceil f(\lceil x \rceil) \rceil$$

Because ceiling is non decreasing

Assume

$$\lceil f(x) \rceil < \lceil f(\lceil x \rceil) \rceil$$

$$\lceil f(x) \rceil < \lceil f(\lceil x \rceil) \rceil \rightarrow \lceil f(\lceil x \rceil) \rceil - \lceil f(x) \rceil \geq 1$$

Because ceiling only deals in integers

This means the monotonically increasing function f must increase above $\lceil f(x) \rceil$ in order to make it possible for $\lceil f(\lceil x \rceil) \rceil - \lceil f(x) \rceil \geq 1$. This means that the following two things must be true

$$\forall y \mid x \leq y < \lceil x \rceil$$

$$f(y) = \lceil f(x) \rceil$$

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

$$\lceil f(x) \rceil < \lceil f(\lceil x \rceil) \rceil \text{ and hence } \lceil f(x) \rceil = \lceil f(\lceil x \rceil) \rceil$$