

## [Tutorial] Math note — Möbius inversion

By [Nisiyama\\_Suzune](#), 2 years ago, 

If you've ever taken some lessons on competitive programming, chances are that you have already heard about one of the most famous formulae the Möbius inversion. This article is aimed to provide some basic insight on what is the Möbius inversion, as well as how to apply it in various programming tasks.

## Prerequisite

If you are not familiar with the linear sieve and multiplicative functions, it is recommended that you read about them first here.

I will introduce some frequently used notations and lemmas first.

## Notation

1.  $[P]$  refers to the boolean expression, i.e.  $[P] = 1$  when  $P$  is true, and 0 otherwise.

2.  $\lfloor x \rfloor$  refers to rounding  $x$  down to the nearest integer. Thus  $\lfloor \frac{p}{q} \rfloor$  refers to the integer division.

3.  $d|n$  means that  $d$  can divide  $n$  (without a remainder).

The following functions are all multiplicative functions, where  $p$  is a prime number and  $k$  is a positive integer:

1. The constant function  $\lambda(p^k) = 1$ .

2. The identity function  $\lambda(p^k) = p^k$ .

3. The power function  $\lambda(p^k) = p^{ak}$ , where  $a$  is constant.

4. The unit function  $\lambda(p^k) = [p^k = 1]$ .

5. The divisor function  $\lambda(p^k) = \sum_{d|p^k} d$ , denoting the sum of the  $d$ -th powers of all the positive divisors of the number.

6. The Möbius function  $\mu(p^k) = [k = 0] - k$ .

7. The Euler's totient function  $\phi(p^k) = p^k - p^{k-1}$ .

## Lemma

I have some my unofficial names for these frequently used conclusions. If you happen to know any more commonly used name for them, you are more than welcome to tell me:

• (**The integer division lemma**) For every positive integer  $p, q$  and  $r$ ,  $\lfloor \frac{p}{q} \rfloor = \lfloor \frac{p-r}{q} \rfloor$ .

Proof: We know that  $\frac{p}{q} - \lfloor \frac{p}{q} \rfloor < 1$ . Hence  $\frac{p-r}{q} - \lfloor \frac{p-r}{q} \rfloor < 1$ . Since the fraction part of  $\frac{p-r}{q}$  cannot exceed  $\frac{r}{q} < 1$ , we achieve the conclusion.

• (**The harmonic lemma**) Consider the harmonic sequence on integer division  $(\lfloor \frac{1}{1}, \lfloor \frac{1}{2}, \dots, \lfloor \frac{1}{n} \rfloor)$ .

1. The sequence is non-increasing, and there are at most  $2\sqrt{n}$  different elements.

2. The sum of the sequence is approximately to  $O(n \log n)$ .

Proof: Denote  $d(i) = \lfloor \frac{1}{i} \rfloor$ . For every  $i$  not exceeding  $\sqrt{n}$ , there will be no more than  $\sqrt{n}$  values in the domain of  $d(i)$ , so there can be at most  $\sqrt{n}$  different values for  $d(i)$ . For the rest part of  $i$  greater than  $\sqrt{n}$ , we can infer that  $d(i) < \sqrt{n}$  and  $i$  is a positive integer, so there can be at most  $2\sqrt{n}$  different values for  $d(i)$ . Therefore we know that there are at most  $2\sqrt{n}$  different elements in the sequence.

Since the Euler-Mascheroni constant states that  $\lim_{n \rightarrow \infty} \sum_{i=1}^n \frac{1}{i} = \ln n + \gamma$ , we know that  $\lim_{n \rightarrow \infty} \sum_{i=1}^n \frac{1}{i} = n \ln n + n\gamma$ , so the sum of the original sequence is approximate to  $O(n \log n)$ .

Moreover, it is actually possible to exploit the property that the sequence has at most  $2\sqrt{n}$  different elements, and write a loop that runs in  $O(\sqrt{n})$  complexity to iterate through every possible value of  $d(i)$ , using the fact that the greatest integer  $x$  satisfying  $d(x) = d(i)$  is  $\lfloor \frac{1}{d(i)} \rfloor$ . The piece of code demonstrates one way to program it.

for (int i = 1, lca; i < n; i++) {  
 lca = i / (n / i);  
 // i / lca yields the same value for i <= x <= lca;  
}

• (**The transitive property of multiplicative functions**)

1. If both  $f(x)$  and  $g(x)$  are multiplicative, then  $f \circ g(x)$  is also multiplicative.

2. If both  $f(x)$  and  $g(x)$  are multiplicative, then their Dirichlet convolution  $f * g(x) = \sum_{d|x} f(d)g(\frac{x}{d})$  is also multiplicative.

Specifically, if  $f(x)$  is multiplicative,  $h(x) = \sum_{d|x} f(d)$  is also multiplicative.

The proof is more mathematical, which I will skip here.

## What is the Möbius inversion?

According to Wikipedia, the Möbius inversion states that:

$f(g(n)) = \sum_{d|n} f(d)g(\frac{n}{d})$  for every positive integer  $n$ , then  $f(n) = \sum_{d|n} \mu(d)f(\frac{n}{d})$ , where  $\mu(x)$  is the Möbius function, which is multiplicative and satisfies  $\mu(1) = 1, \mu(p) = -1$  for any prime number  $p$  and any integer  $k \geq 2$ . It's worth noting that you can pre-compute all values of the Möbius function from  $l$  to  $n$  using the linear sieve .

However, the definition alone does not mean much (unless the problem statement explicitly gives you something like  $g(n) = \sum_{d|n} f(d)$ ). In that case, we... well... there is one important property that is probably more useful than the definition:

$$\sum_{d|n} \mu(d) = \epsilon(n) = [n = 1]$$

In order to prove this property, we have to use the property of multiplicative functions to show that  $f(n) = \sum_{d|n} \mu(d)f(d)$  is multiplicative. After that, we can see  $f(1) = 1$  and  $f(p) = 0$ , which means  $f(x) = \epsilon(x)$ . Now you may ask: why is this property important? I think it is best to show the reasons in some basic examples below.

Example 1. Find out the number of co-prime pairs of integer  $(x, y)$  in range  $[1, n]$ .

Solution 1. Notice that the question is the same as asking you the value of

$$f(n) = \sum_{i=1}^n \sum_{j=1}^n [\gcd(i, j) = 1].$$

Now apply the Möbius inversion on  $[\gcd(i, j) = 1]$ , we have

$$f(n) = \sum_{i=1}^n \sum_{j=1}^n \sum_{d|\gcd(i, j)} \mu(d)$$

which is the same as

$$f(n) = \sum_{i=1}^n \sum_{j=1}^n \sum_{d=1}^n [d|i, d|j] \mu(d)$$

Notice that  $[d|\gcd(i, j)] = [d|i][d|j]$ . Therefore

$$f(n) = \sum_{i=1}^n \sum_{j=1}^n \sum_{d=1}^n [d|i][d|j] \mu(d)$$

We can change the order of summing things up, so

$$f(n) = \sum_{d=1}^n \mu(d) \left( \sum_{i=1}^n [d|i] \right) \left( \sum_{j=1}^n [d|j] \right)$$

We know that  $\sum_{i=1}^n [d|i] = \sum_{j=1}^n [d|j] = \lfloor \frac{n}{d} \rfloor$ . Thus

$$f(n) = \sum_{d=1}^n \mu(d) \lfloor \frac{n}{d} \rfloor^2$$

Then we can simply loop  $i$  to  $n$  to compute the formula. While we can optimize this loop to  $O(\sqrt{n})$  using the harmonic lemma, we still have to use the linear sieve to pre-compute the values of  $\mu(d)$ . Therefore, the overall complexity of the algorithm is  $O(n \log n)$ .

Example 2. Find out the sum of  $\gcd(x, y)$  for every pair of integer  $(x, y)$  in range  $[1, n]$  ( $\text{lcm}(x, y)$  means the least common multiple of  $x$  and  $y$ ).

Solution 2. Similar as above, notice that the question is the same as asking you the value of

$$f(n) = \sum_{i=1}^n \sum_{j=1}^n [\gcd(i, j) = 1].$$

Let  $k = \gcd(i, j)$ . We can then loop for  $k$  first:

$$f(n) = \sum_{k=1}^n \sum_{i=1}^n \sum_{j=1}^n [\gcd(i, j) = k].$$

Now assume  $i = ak, j = bk$ , and then

$$f(n) = \sum_{k=1}^n \sum_{a=1}^{\lfloor \frac{n}{k} \rfloor} \sum_{b=1}^{\lfloor \frac{n}{k} \rfloor} [\gcd(a, b) = 1]$$

It can be observed that the last part of the formula is the same as the one in example 1. Applying the same procedure, we have

$$f(n) = \sum_{k=1}^n \sum_{d=1}^{\lfloor \frac{n}{k} \rfloor} \sum_{d|k} \mu(d) \lfloor \frac{n}{kd} \rfloor^2$$

According to the harmonic lemma,  $O(\sum_{k=1}^n \lfloor \frac{n}{k} \rfloor) = O(n \log n)$ . Therefore, if we compute the sum above with brute force, the overall complexity will be  $O(n \log n)$ .

This is, however, not the best complexity we can achieve with the Möbius inversion. Now let  $l = kd$ , and we can loop for  $l$  first:

$$f(n) = \sum_{l=1}^n \sum_{d=1}^{\lfloor \frac{n}{l} \rfloor} \sum_{d|l} \mu(d) \lfloor \frac{n}{l} \rfloor^2$$

Applying the transitive property of multiplicative functions, we can see that  $g(l) = \sum_{d|l} \mu(d)\lfloor \frac{n}{l} \rfloor$  is multiplicative. Moreover, we have  $g(p^k) = p^k - p^{k-1}$ . If you have somewhat studied about the number theory, you may figure out that  $g(l)$  is actually the Euler's totient function. Regarding of whether you know about the condition or not,  $g(l)$  can be pre-computed with the linear sieve, and  $f(n) = \sum_{l=1}^n g(l)$ .

Example 3. Find out the sum of  $\text{lcm}(x, y)$  for every pair of integer  $(x, y)$  in range  $[1, n]$  ( $\text{lcm}(x, y)$  means the least common multiple of  $x$  and  $y$ ).

Solution 3. Well, we should be pretty familiar with the techniques by now. First of all, the answer should be

$$f(n) = \sum_{i=1}^n \sum_{j=1}^n \text{lcm}(i, j)$$

Since  $\text{lcm}(i, j) = \frac{ij}{\gcd(i, j)}$ , let  $k = \gcd(i, j)$ . We can then loop for  $k$  first:

$$f(n) = \sum_{k=1}^n \sum_{i=1}^n \sum_{j=1}^n [\gcd(i, j) = k]$$

Now assume  $i = ak, j = bk$ , and then

$$f(n) = \sum_{k=1}^n \sum_{a=1}^{\lfloor \frac{n}{k} \rfloor} \sum_{b=1}^{\lfloor \frac{n}{k} \rfloor} [\gcd(a, b) = 1]$$

It can be observed that the last part of the formula is the same as the one in example 1. Applying the same procedure, we have

$$f(n) = \sum_{k=1}^n \sum_{d=1}^{\lfloor \frac{n}{k} \rfloor} \sum_{d|k} \mu(d) \lfloor \frac{n}{kd} \rfloor^2$$

According to the harmonic lemma,  $O(\sum_{k=1}^n \lfloor \frac{n}{k} \rfloor) = O(n \log n)$ . Therefore, if we compute the sum above with brute force, the overall complexity will be  $O(n \log n)$ .

This editorial might also help, although it does not use the Möbius function. That's it, hope I helped!

→ back

</div