7. Möbius inversion formula

To read:
[5] Chapter 2.1.

Definition 7.1. Suppose that a positive integer n has the prime factorization

$$n = p_1^{e_1} \cdots p_r^{e_r}.$$

We define the *Möbius function* $\mu(n)$ as:

$$\mu(n) = \begin{cases} 1 \ \text{ for } \ n = 1, \\ 0 \text{ if some } \ e_i > 1, \\ (-1)^r \text{ if } e_1 = \ldots = e_r = 1. \end{cases}$$

Lemma 7.2. *For $n \in \mathbb{Z}_{\geq 1}$ we have*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 \ \text{ if } \ n = 1, \\ 0 \ \text{ if } \ n > 1. \end{cases}$$

Here the summation is taken over all positive divisors on n.

Proof. First consider the case $n = 1$. It follows immediately from the definition

$$\sum_{d|1} \mu(d) = \mu(1) = 1.$$

Next, suppose that $n > 1$ and it has the prime decomposition $n = p_1^{e_1} \cdots p_r^{e_r}$. Set $n^* := p_1 \cdots p_r$. If $d \mid n$ and $d \nmid n^*$ then d has a prime divisor of multiplicity bigger then 1 and therefore $\mu(d) = 0$. Hence, we have

$$\sum_{d|n} \mu(d) = \sum_{d|n^*} \mu(d).$$

Now we can easily compute

$$\sum_{d|n^*} \mu(d) = 1 - \binom{r}{1} + \binom{r}{2} - \binom{r}{3} + \ldots = (1-1)^r = 0.$$

This finishes the proof. □

Theorem 7.3. *(Möbius inversion formula) Let functions $f, g : \mathbb{Z}_{\geq 1} \to \mathbb{R}$ be such that*

$$f(n) = \sum_{d|n} g(d).$$

Then

$$g(n) = \sum_{d|n} \mu(d)\, f(n/d).$$

Proof. We have

$$f(n/d) = \sum_{d'|(n/d) g(d')} \quad \text{for all } d \mid n.$$

Therefore

$$\sum_{d|n} \mu(d)\, f(n/d) = \sum_{d|n} \mu(d) \sum_{d'|(n/d)} g(d').$$

Let $n = dd'n_1$. For a fixed d', the value of d runs over all positive divisors of n/d'. Hence we get

$$\sum_{d|n} \mu(d) \sum_{d'|(n/d)} g(d') = \sum_{d'|n} g(d') \sum_{d|(n/d')} \mu(d).$$

We apply the previous lemma to the sum $\sum_{d|(n/d')} \mu(d)$ and obtain

$$\sum_{d'|n} g(d') \sum_{d|(n/d')} \mu(d) = g(n).$$

This finishes the proof. □

7.1. **Identities with Euler's totient function.**

Exercise 6. Show that for all $n \in \mathbb{Z}_{\geq 1}$ we have

$$n = \sum_{d|n} \phi(d).$$

Hint: Let Φ_n be the set all elements in $[n]$ coprime to n:

$$\Phi_n := \{m \in [n] \mid m \text{ is coprime to } n\}.$$

Show that $[n]$ is the disjoint union of sets $(n/d) \cdot \Phi_d$ where d runs over all divisors of n:

$$[n] = \dot{\bigcup}_{d|n} (n/d) \cdot \Phi_d.$$

Exercise 7. Show that $\phi(n) = n \sum_{d|n} \frac{\mu(d)}{d}$.

7.2. **Number of cyclic sequences.**

Definition 7.4. Let A be a set. A *linear sequence* of length n on an A is a sequence of the form

$$(a_1, \ldots, a_n), \quad a_k \in A \text{ for } k = 1, \ldots n.$$

In other words, a linear sequence is a function $a : [n] \to A$.

The number of linear sequences of length n on an alphabet of size r is r^n.

Consider the following equivalence relation $\sim$ on the set of linear sequences:

$$(a_1, ..., a_n) \sim (a_1, ..., a_n)$$

and

$$(a_1, ..., a_n) \sim (a_k, a_{k+1}, \ldots, a_1, \ldots, a_{k-1}), \quad k = 2, \ldots n.$$

In other words, two linear sequences are equivalent if one of them can be obtained from another by a cyclic shift.

Example. Linear sequences of length 3 on the alphabet $\{a, b\}$:

$$(a, a, a)$$
$$(a, a, b)$$
$$(a, b, a)$$
$$(a, b, b)$$
$$(b, a, a)$$
$$(b, a, b)$$
$$(b, b, a)$$
$$(b, b, b).$$

Cyclic sequences of length 3 on the alphabet $\{a, b\}$:

$$
\begin{aligned}
&(a, a, a)\\
&(a, a, b) \sim (a, b, a) \sim (b, a, a)\\
&(a, b, b) \sim (b, b, a) \sim (b, a, b)\\
&(b, b, b).
\end{aligned}
$$

Definition 7.5. A *cyclic sequence* of length n on an alphabet A is an equivalence class of linear sequences with respect to the relation $\sim$.

Proposition 7.6. *The number $T(n, r)$ of cyclic sequences of of length n on an alphabet of size r is*

$$T(n, r) = \frac{1}{n} \sum_{d|n} \phi(n/d) r^d.$$

Proof. A *period* of a cyclic sequence $(a_1, \ldots, a_n)$ is a minimal number $k \in \{1, 2, \ldots, n\}$ such that $(a_1, \ldots, a_n) = (a_{1+k}, \ldots, a_n, a_1, \ldots a_k)$ (equal as linear sequences). Note that the period of a sequence is a divisor of the the sequence's length.

Let $M(d, r)$ be the number of cyclic sequences of of length d and period exactly d. It is easy to see that

$$r^n = \sum_{d|n} d\, M(d, r).$$

The Möbius inversion formula implies

$$n\, M(n, r) = \sum_{d|n} \mu(d/n)\, r^d. \tag{4}$$

We have

$$T(n, r) = \sum_{d|n} M(d, r).$$

We combine this identity with (4) and obtain

$$
\begin{aligned}
T(n, r) =& \sum_{d|n} \frac{1}{d} \sum_{d'|d} \mu(d'/d)\, r^{d'}\\
& \qquad \text{(here we intoduce a new summation variable } d'' = \frac{d}{d'})\\
=& \sum_{d'|n} r^{d'} \left(\sum_{d''|\frac{n}{d'}} \frac{1}{d'd''}\, \mu(d'') \right).
\end{aligned}
$$

Now we use the identity

$$\sum_{d''|\frac{n}{d'}} \frac{1}{d''}\, \mu(d'') = \frac{\phi(n/d')}{n/d'}$$

and arrive at

$$
\begin{aligned}
T(n, r) =& \sum_{d'|n} r^{d'}\, \frac{1}{d'}\, \frac{\phi(n/d')}{n/d'}\\
=& \frac{1}{n} \sum_{d'|n} \phi(n/d')\, r^{d'}.
\end{aligned}
$$

This finishes the proof. □