Möbius Inversion Formula

Theorem : Möbius Inversion Formula

Let f and g be arithmetic functions. Then

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

If and only if

$$g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) f(d)$$

Proof. Assume that $f(n) = \sum_{d|n} g(d)$. Then

$$\begin{aligned}\sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) &= \sum_{d|n} \left(\mu(d) \sum_{c|\frac{n}{d}} g(c)\right) \\ &= \sum_{c|n} \left(g(c) \sum_{d|\frac{n}{c}} \mu(d)\right)\end{aligned}$$

By Corollary 9.7, the summation inside the parentheses is 0 unless

$$\frac{n}{c} = 1 \quad \text{or equivalently} \quad n = c$$

The only contribution of the outer summation is when $c = n$ giving

$$\sum_{d} \mu(d) f\left(\frac{n}{d}\right) = g(n)$$

Assume that $g(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) f(d)$. Then

$$\begin{aligned}\sum_{d|n} g(d) &= \sum_{d|n} \left(\sum_{c|d} \mu\left(\frac{d}{c}\right) f(c)\right) \\ &= \sum_{c|n} \left(f(c) \sum_{d|c} \mu\left(\frac{d}{c}\right)\right) \\ &= \sum_{c|n} \left(f(c) \sum_{m|\frac{n}{c}} \mu(m)\right)\end{aligned}$$

By Corollary 9.7, the summation inside the parentheses is 0 unless

$$\frac{n}{c} = 1 \quad \text{or equivalently} \quad n = c$$

The only contribution of the outer summation is when $c = n$ giving

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

□

Example

Let $g(n) = n$ for all $n \in \mathbb{Z}$ with $n > 0$. By Gauss' Theorem, we have

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

Apply the Möbius Inversion Formula to obtain a nontrivial identity.

Applying the Möbius Inversion Formula gives us:

$$\begin{aligned}\phi(n) &= \sum_{d|n} \mu(d)\, g\left(\frac{n}{d}\right) \\ &= \sum_{d|n} \mu(d)\, \frac{n}{d} \\ &= \sum_{d|n} \mu\left(\frac{n}{d}\right) d\end{aligned}$$

Example

Verify for $n = 12$ that

$$\phi(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) d$$

The divisors of 12 are 1, 2, 3, 4, 6, and 12. Therefore we have that:

$$\begin{aligned}\sum_{d|n} \mu\left(\frac{n}{d}\right) d &= \mu(12)\cdot 1 + \mu(6)\cdot 2 + \mu(4)\cdot 3 + \mu(3)\cdot 4 + \mu(2)\cdot 6 + \mu(1)\cdot 12 \\ &= 0\cdot 1 + 1\cdot 2 + 0\cdot 3 - 1\cdot 4 - 1\cdot 6 + 1\cdot 12 \\ &= 4 \\ &= \phi(12)\end{aligned}$$

Example

Let $v(n) = 1$ for all $n \in \mathbb{Z}$ with $n > 0$, We have that

$$d(n) \sum_{d|n} v(d)$$

Apply the Möbius Inversion Formula to obtain a nontrivial identity.

By the Möbius Inversion Formula, we obtain the nontrivial identity

$$\begin{aligned} 1 &= \sum_{d|n} \mu(d)\, d\left(\frac{n}{d}\right) \\ &= \sum_{d|n} \mu\left(\frac{n}{d}\right) d(d) \end{aligned}$$

Example

Verify for $n = 12$ that

$$1 = \sum_{d|n} \mu\left(\frac{n}{d}\right) d(d)$$

The divisors of 12 are 1, 2, 3, 4, 6, and 12. Therefore we have that

$$\begin{aligned} \sum_{d|n} \mu\left(\frac{n}{d}\right) d(d) &= \mu(12)\cdot 1 + \mu(6)\cdot 2 + \mu(4)\cdot 2 + \mu(3)\cdot 3 + \mu(2)\cdot 4 + \mu(1)\cdot 6 \\ &= 0\cdot 1 + 1\cdot 2 + 0\cdot 2 - 1\cdot 3 - 1\cdot 4 + 1\cdot 6 \\ &= 1 \end{aligned}$$

Example

Let $g(n) = n$ for all $n \in \mathbb{Z}$ with $n > 0$. By definition of $\sigma(n)$ we have

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

Apply the Möbius Inversion Formula to obtain a nontrivial identity.

By the Möbius Inversion Formula, we obtain the nontrivial identity

$$\begin{aligned} n &= \sum_{d} \mu(d)\, \sigma\left(\frac{n}{d}\right) \\ &= \sum_{d} \mu\left(\frac{n}{d}\right) \sigma(d) \end{aligned}$$

Example

Verify for $n = 12$ that

$$n = \sum_{d} \mu(d)\, \sigma\left(\frac{n}{d}\right)$$

The divisors of 12 are 1, 2, 3, 4, 6, and 12. Therefore we have that

$$\begin{aligned}\sum_{d} \mu\left(\frac{n}{d}\right) \sigma(d) &= \mu(12) \cdot 1 + \mu(6) \cdot 3 + \mu(4) \cdot 4 + \mu(3) \cdot 7 + \mu(2) \cdot 12 + \mu(1) \cdot 28 \\ &= 0 \cdot 1 + 1 \cdot 3 + 0 \cdot 4 - 1 \cdot 7 - 1 \cdot 12 + 1 \cdot 28 \\ &= 12\end{aligned}$$

Example

Let $\mathbb{F}_q$ be the finite field with q elements and let $f(n)$ be the number of monic irreducible polynomials of degree n. Apply the Möbius inversion formula to count the number of irreducible polynomials of degree n that exist over $\mathbb{F}_q$ if the following polynomial has q^n distinct roots.

$$X^{q^n} - X \in \mathbb{F}_q[X]$$

Each degree n polynomial can be decomposed according to the degrees of its irreducible factors, so

$$\sum_{d \mid n} d f(d) = q^n$$

By the Möbius Inversion Formula, we obtain the nontrivial identity

$$f(n) = \frac{1}{n} \sum_{d \mid n} \mu(d)\, q^{n/d}$$

If $q = 5$ and $n = 2$, then the number of irreducible polynomials is given by

$$f(2) = \frac{1}{2} \sum_{d \mid 2} \mu(d) \cdot 5^{2/d} = \frac{1}{2}\left(5^2 - 5\right) = 10$$

The list of these polynomials are

$$x^2 + x + 1, \quad x^2 + 4x + 1, \quad x^2 + 2, \quad x^2 + x + 2, \quad x^2 + 4x + 2,$$

$$x^2 + 3, \quad x^2 + 2x + 3, \quad x^2 + 3x + 3, \quad x^2 + 2x + 4, \quad x^2 + 3x + 4$$

Definition : The Riemann Hypothesis

Conjecture: All non-trivial zeros of the Riemann zeta function $\zeta(s)$ lie on the critical line $\mathrm{Re}(s) = \frac{1}{2}$.

The Riemann Hypothesis is equivalent to a strong bound on the partial sums of the Möbius function.

$$M(x) = \sum_{n \leq x} \mu(n) = O^{\left(x^{\frac{1}{2}+\epsilon}\right)}$$

Definition : Mertens Conjecture

Conjecture: For all $x > 1$, we have that

$$|M(x)| = \sqrt{x}$$

This was disproved by Odlyzko and Riele in 1985. However, no explicit counterexample is known.

Definition : Chowla Conjecture

Conjecture: For any distinct positive integers $k_1, \ldots, k_n$,

$$\sum_{n} \mu(n + k_1)\,\mu(n + k_2) \ldots \mu(n + k_n) = o(x)$$

This conjecture states that values of $\mu(n)$ behave pseudo randomly and are asymptotically uncorrelated.