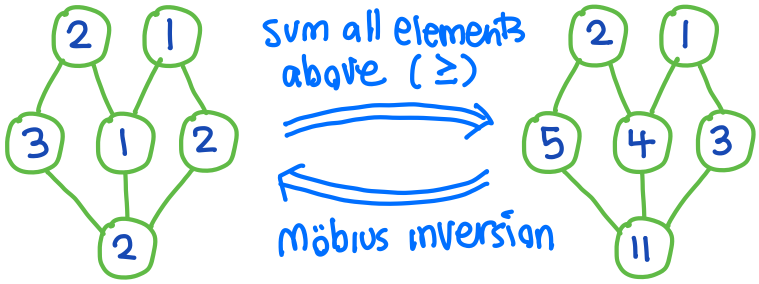
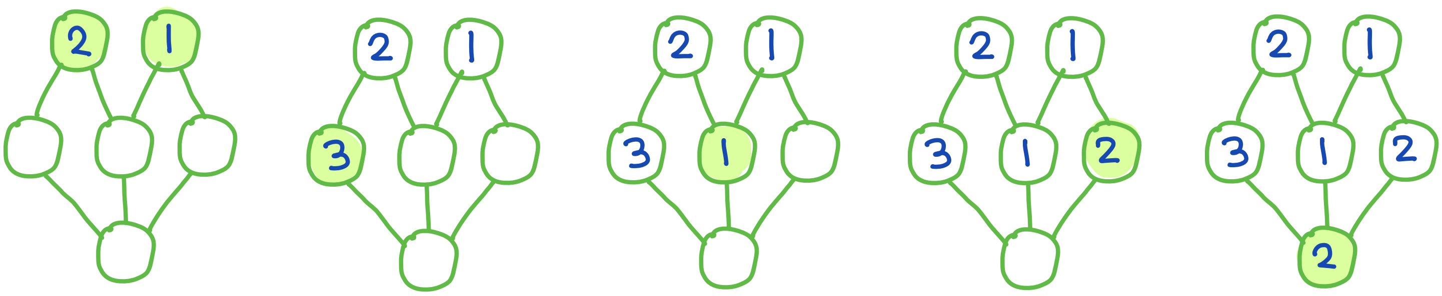
Möbius inversion and cyclotomic polynomials

For any poset, Möbius inversion is inverse to partial sums:

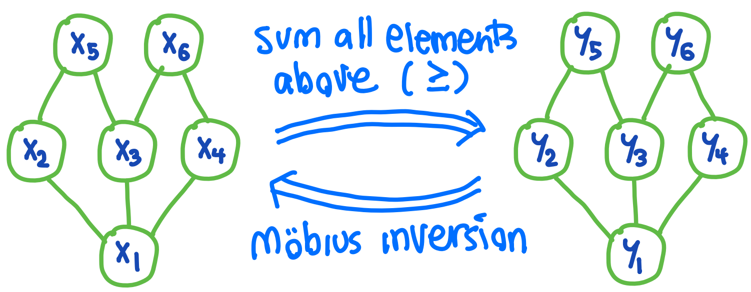


One can carry out the inversion incrementally, correcting each partial sum by summing the values strictly above:



(The theory is identical if one is instead summing below.)

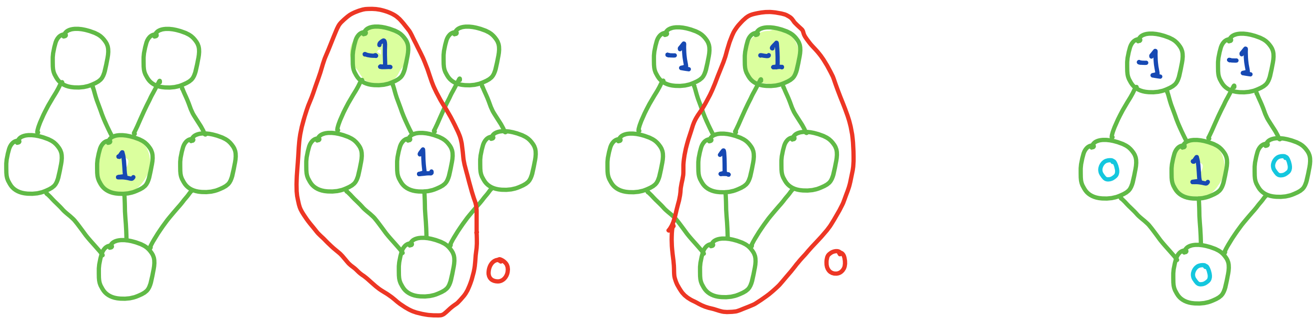
Partial sums is a linear map; Möbius inversion is its inverse:



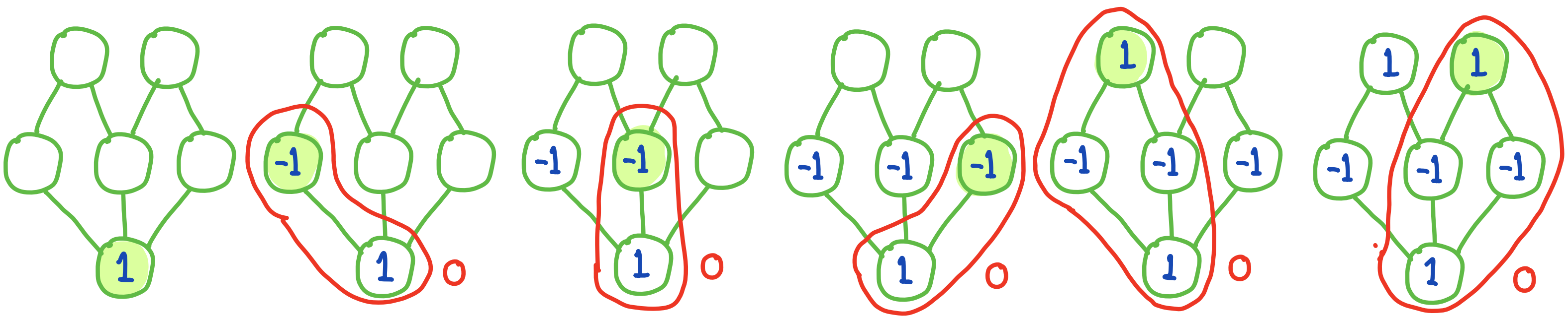
$$\begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ & 1 & 0 & 0 & 1 & 0 \\ & & 1 & 0 & 1 & 1 \\ & & & 1 & 0 & 1 \\ & & & & 1 & 0 \\ & & & & & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{bmatrix} \qquad \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 & -1 & -1 \\ & 1 & 0 & 0 & -1 & 0 \\ & & 1 & 0 & -1 & -1 \\ & & & 1 & 0 & -1 \\ & & & & 1 & 0 \\ & & & & & 1 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \end{bmatrix}$$

sum all elements above (≥) Möbius inversion

Each row of this inverse can be computed incrementally.
Start with a 1 at the desired entry, then work up the poset so all coefficient partial sums below are zero.

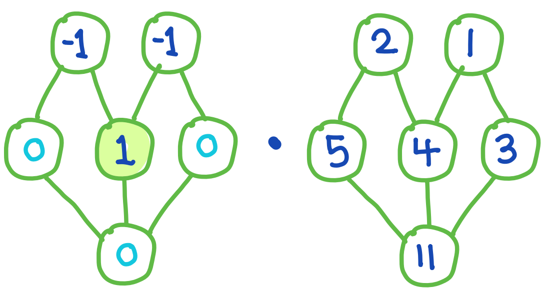


Coefficients for x_4 are $[0\ 0\ 1\ 0\ {-1}\ {-1}]$

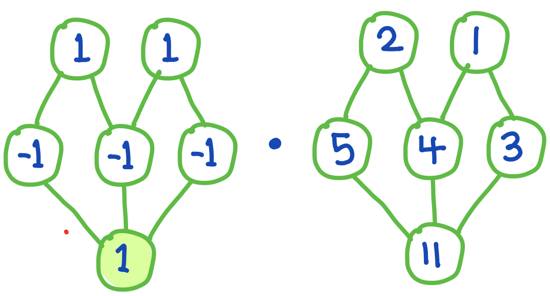


Coefficients for x_1 are $[1\ {-1}\ {-1}\ {-1}\ 1\ 1]$

We can use these coefficients to directly invert the partial sums:



$$= [0\ 0\ 1\ 0\ {-1}\ {-1}]\begin{bmatrix}11\\5\\4\\3\\2\\1\end{bmatrix} = 1 = x_4$$



$$= [1\ {-1}\ {-1}\ {-1}\ 1\ 1]\begin{bmatrix}11\\5\\4\\3\\2\\1\end{bmatrix} = 2 = x_1$$

In many applications one can find these coefficients by other means than direct matrix inversion.

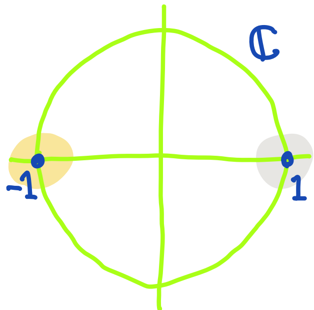
For example, there are often homological* methods.

* algebraic topology

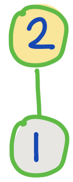
Cyclotomic polynomials

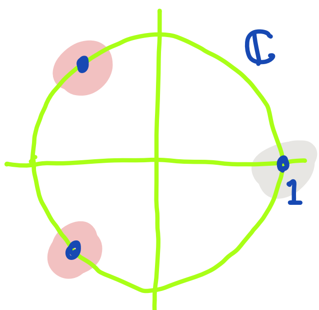
The n^{th} roots of unity are the roots of $x^n - 1 = 0$.

Each $x^n - 1$ has a factorization into distinct irreducible polynomials with integer coefficients, called cyclotomic polynomials.

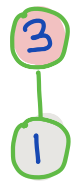


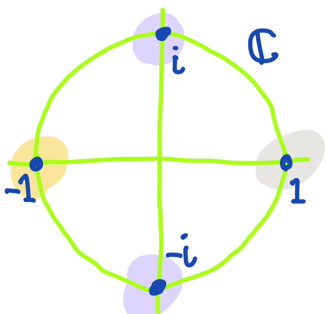
$$x^2 - 1 = (x-1)(x+1)$$



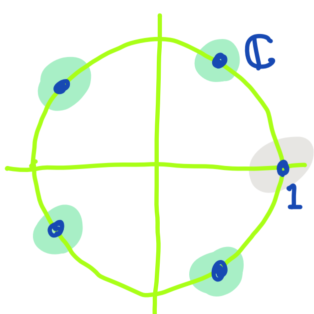


$$x^3 - 1 = (x-1)(x^2+x+1)$$

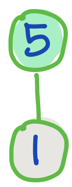


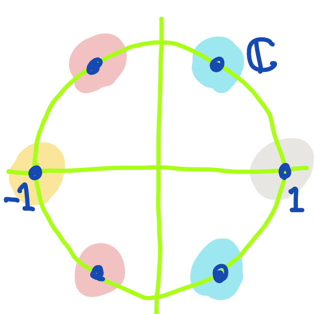


$$x^4 - 1 = (x-1)(x+1)(x^2+1)$$

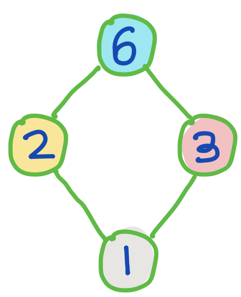


$$x^5 - 1 = (x-1)(x^4+x^3+x^2+x+1)$$



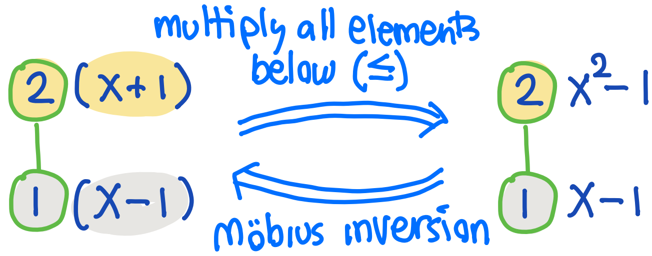


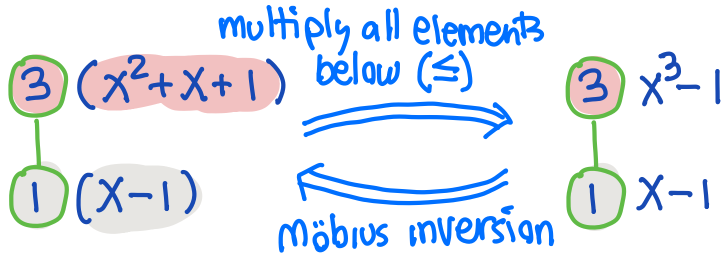
$$x^6 - 1 = (x-1)(x+1)(x^2+x+1)(x^2-x+1)$$

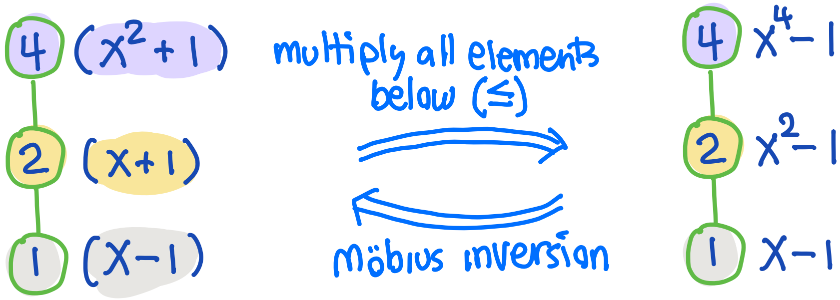


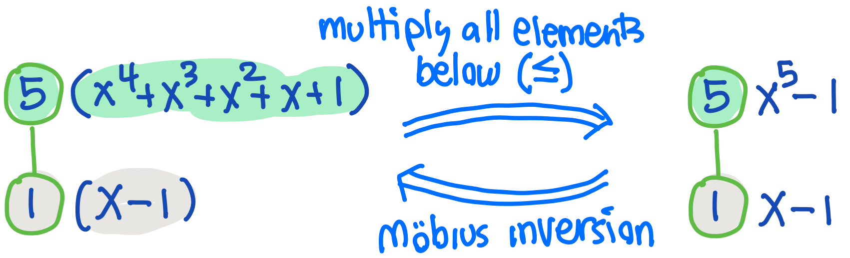
The divisor lattice of n is the poset of integer factors of n, partially ordered by divisibility.

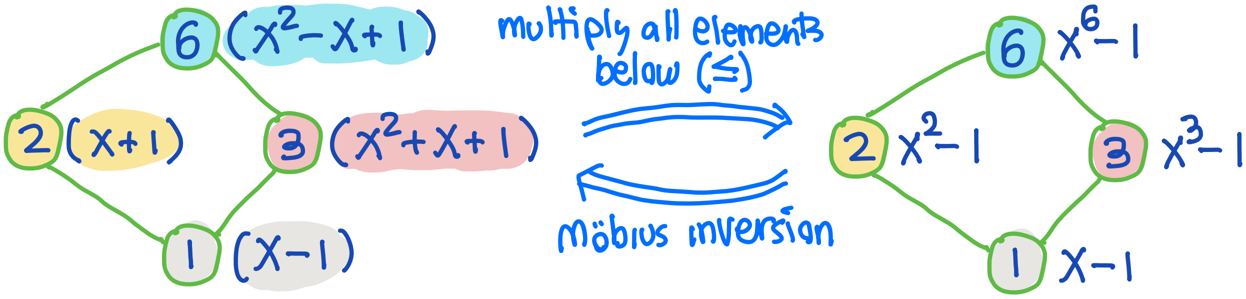
As seen above, the cyclotomic polynomials that are factors of x^n-1 correspond to the elements of the divisor lattice.
The polynomials x^d-1 for each factor d of n appear as partial products of the cyclotomic polynomials for each factor e of d.
We recognize this as a form of Möbius inversion, with sum replaced by product, and ascending rather than descending partial products:











This gives effective algorithms for computing cyclotomic polynomials.