1 | base knowlege

1.1 | primitive root of unity

1.1.1 | a number r is a primitive nth root of unity iff n is the smallest counting number for which $r^n = 1$.

1.1.2 | `https://mathworld.wolfram.com/PrimitiveRootofUnity.html` source

1.2 | convolution theorem

1.2.1 | 'depends fundamentally on the convolution theorem, which provides an efficient way to compute the cyclic convolution of two sequences. It states that the cyclic convolution of two vectors can be found by taking the discreate fourier transform of each of them, multiplying the resulting vectors element by element, and then taking the inverse discrete fourier transform.'

2 | sources

2.1 | explanation of multiplication algorithm