

1. $L^2(\mathbb{Z}_n)$ is a ring of n dimensional vectors where each element is complex.
 $*$ is defined as convolution which is

$$(f * g)(k) = \sum_{i+j \equiv k \pmod n} f(i)g(j) \quad (1)$$

Now, let us prove for f, g, j that they are associative
our theorem is

$$(f * g) * j = f * (g * j) \quad (2)$$

on the right hand side, let us say we have a number k where for each group in t groups of indices in f, g , and j it is equivalent to the sum mod n . We will show these indices as $(i_0, i_1, i_2), (i_3, i_4, i_5), \dots, (i_{3t}, i_{3t+1}, i_{3t+2})$. So the sum of $i_{3m} + i_{3m+1} + i_{3m+2} \equiv k \pmod n$ for all $m \in \mathbb{Z}$ from 0 to $3t + 2$.

Now, on the rhs, we do $f * g$ then on index $i_{3m} + i_{3m+1} \pmod n$ we would have a sum of $f(i_{3m})g(i_{3m+1})$ that maps to that index. Now, when we convolve this by j , since

$$i_{3m} + i_{3m+1} \pmod n + i_{3m+2} \equiv k \pmod n \quad (3)$$

we'll have the sum of all $f(i_{3m})g(i_{3m+1})j(i_{3m+2})$ mapping to index k . We can do the same argument on rhs using $i_{3m+1} + i_{3m+2} \pmod n$. Thus, associativity holds.

2.

Given $a = (a_0, a_1, a_2)$ and $b = (b_0, b_1, b_2)$, $a * b$ is

$$(a_0b_0 + a_2b_1 + a_1b_2, a_1b_0 + a_0b_1 + a_2b_2, a_2b_0 + a_1b_1 + a_0b_2) \quad (4)$$

Now, we can make a matrix multiplication to produce this result as so

$$\begin{pmatrix} a_0 & a_2 & a_1 \\ a_1 & a_0 & a_2 \\ a_2 & a_1 & a_0 \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \end{pmatrix} \quad (5)$$

3.

We can make the above matrix by

$$a_0 \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} + a_1 \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} + a_2 \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \quad (6)$$

4.

Given $\omega = e^{\frac{2\pi i}{n}}$, the fourier matrix F_3 is (in 3×3)

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega^4 \end{pmatrix} \quad (7)$$

This written in terms of e is

$$\begin{pmatrix} 1 & 1 & 1 \\ & \frac{2\pi i}{3} & \frac{2\pi i}{3} \\ 1 & e^{\frac{2\pi i}{3}} & e^{\frac{2\pi i}{3}} \\ & \frac{2\pi i}{3} & \frac{2\pi i}{3} \\ 1 & e^{\frac{2\pi i}{3}} & e^{\frac{2\pi i}{3}} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ & \frac{2\pi i}{3} & \frac{\pi i}{3} \\ 1 & e^{\frac{2\pi i}{3}} & e^{\frac{\pi i}{3}} \\ & \frac{\pi i}{3} & \frac{2\pi i}{3} \\ 1 & e^{\frac{\pi i}{3}} & e^{\frac{2\pi i}{3}} \end{pmatrix} \quad (8)$$

Now F_3^* is

$$\begin{pmatrix} 1 & 1 & 1 \\ & -\frac{2\pi i}{3} & -\frac{2\pi i}{3} \\ 1 & e^{\frac{-2\pi i}{3}} & e^{\frac{-2\pi i}{3}} \\ & -\frac{2\pi i}{3} & -\frac{2\pi i}{3} \\ 1 & e^{\frac{-2\pi i}{3}} & e^{\frac{-2\pi i}{3}} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ & \frac{\pi i}{3} & \frac{2\pi i}{3} \\ 1 & e^{\frac{\pi i}{3}} & e^{\frac{2\pi i}{3}} \\ & \frac{2\pi i}{3} & \frac{\pi i}{3} \\ 1 & e^{\frac{2\pi i}{3}} & e^{\frac{\pi i}{3}} \end{pmatrix} \quad (9)$$

Now when we multiply along the diagonal, it is pretty clear that we get 3s. But what about the other locations? Interestingly, they all seem to cancel out. For example, if we are summing with the one vectors, along any column or row except the diagonal, the sum is always 0 as the complex parts cancel out and the real part for both cancel out with one too as each have a -0.5 component.

If we are not multiplying by the one vector then we get the same situation as above regardless. I don't think I can prove this in the general case but it turns out when you multiply them you get 3 times the identity.

5. The obvious case is $S_3 = D_3 = I$. But I don't think that's the intention. Let us test out with

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \quad (10)$$

This will result in

$$\begin{pmatrix} 1 & 1 & 1 \\ \omega^2 & 1 & \omega \\ \omega^4 & 1 & \omega^2 \end{pmatrix} \quad (11)$$

Now, as $FS = DF$, let's multiply both sides by $1/3F^*$ then we have $D = F S F^{-1}$. This is the same as

$$\frac{1}{3} \begin{pmatrix} 1 & 1 & 1 \\ e^{\frac{2\pi i}{3}} & 1 & e^{\frac{2\pi i}{3}} \\ e^{\frac{4\pi i}{3}} & 1 & e^{\frac{2\pi i}{3}} \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 1 & e^{\frac{\pi i}{3}} & e^{\frac{2\pi i}{3}} \\ 1 & e^{\frac{2\pi i}{3}} & e^{\frac{\pi i}{3}} \end{pmatrix} \quad (12)$$

$$= \frac{1}{3} \begin{pmatrix} 1 & 1 & 1 \\ e^{\frac{\pi i}{3}} & 1 & e^{\frac{2\pi i}{3}} \\ e^{\frac{2\pi i}{3}} & 1 & e^{\frac{\pi i}{3}} \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 1 & e^{\frac{\pi i}{3}} & e^{\frac{2\pi i}{3}} \\ 1 & e^{\frac{2\pi i}{3}} & e^{\frac{\pi i}{3}} \end{pmatrix} \quad (13)$$

$$= \begin{pmatrix} 1 & 0 & 0 \\ 0 & e^{\frac{\pi i}{3}} & 0 \\ 0 & 0 & e^{\frac{2\pi i}{3}} \end{pmatrix} \quad (14)$$

$$= \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix} \quad (15)$$

wow this is interesting. This does show that

$$FCF^{-1} \quad (16)$$

yields a diagonal matrix as

$$C = a_0 S_0 + a_1 S_1 + a_2 S_2 \quad (17)$$

and as

$$FS_i F^{-1} = D_i \quad (18)$$

then

$$FCF^{-1} = a_0 D_0 + a_1 D_1 + a_2 D_2 \quad (19)$$

which is a diagonal matrix. 6.

$$C(a) * b = a * b \quad (20)$$

$$\begin{pmatrix} a_0 & a_2 & a_1 \\ a_1 & a_0 & a_2 \\ a_2 & a_1 & a_0 \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} a_0 b_0 + a_2 b_1 + a_1 b_2 \\ a_1 b_0 + a_0 b_1 + a_2 b_2 \\ a_2 b_0 + a_1 b_1 + a_0 b_2 \end{pmatrix} \quad (21)$$

Now, let's add rotated columns

$$\begin{pmatrix} a_0 & a_2 & a_1 \\ a_1 & a_0 & a_2 \\ a_2 & a_1 & a_0 \end{pmatrix} \begin{pmatrix} b_0 & b_1 & b_2 \\ b_1 & b_2 & b_0 \\ b_2 & b_0 & b_1 \end{pmatrix} = \begin{pmatrix} a_0 b_0 + a_2 b_1 + a_1 b_2 & a_1 b_0 + a_0 b_1 + a_2 b_2 & a_2 b_0 + a_1 b_1 + a_0 b_2 \\ a_1 b_0 + a_0 b_1 + a_2 b_2 & a_2 b_0 + a_1 b_1 + a_0 b_2 & a_0 b_0 + a_2 b_1 + a_1 b_2 \\ a_2 b_0 + a_1 b_1 + a_0 b_2 & a_0 b_0 + a_2 b_1 + a_1 b_2 & a_1 b_0 + a_0 b_1 + a_2 b_2 \end{pmatrix} \quad (22)$$

Thus we found the matrices. 7. $x - 1$ and $x^2 + x + 1$ doesn't have common factors. So

$$\gcd(x - 1, x^2 + x + 1) = 1 \quad (23)$$

$$\frac{1}{3}((x - 1)(-x - 2) + (x^2 + x + 1)) = 1 \quad (24)$$

Now,

$$1 + (x - 1)p(x) = x + 1 + (x^2 + x + 1)q(x) \quad (25)$$

so we have

$$(x - 1)p(x) - (x^2 + x + 1)q(x) = x \quad (26)$$

from the above we get the solution as

$$(x - 1)(x/3 + 2/3)x - (x^2 + x + 1)x/3 = x \quad (27)$$

so

$$f = x^3/3 + x^2/3 + x/3 + x + 1 \quad (28)$$

8.

$$x^2 + 1 \pmod{x^3 - 1} \quad (29)$$

is in the ring

$$\frac{C[x]}{x^3 - 1} \quad (30)$$

Now, to work with the Fourier transform we need to work with vectors. We can think of $x^2 + 1$ as

$$a = \begin{pmatrix} 1 & 0 & 1 \end{pmatrix} \quad (31)$$

which when multiplied with

$$\begin{pmatrix} 1 \\ x \\ x^2 \end{pmatrix} \quad (32)$$

gives our polynomial.

polynomial multiplication is the same as vector convolution in this space. We want to find $b(x)$ such that

$$(x^2 + 1)b(x) \equiv 1 \pmod{x^3 - 1} \quad (33)$$

This means we want to find a matrix b such that

$$a * b = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix} = c \quad (34)$$

From the convolution theorem we know that the convolution of two elements before Fourier transform is the the same as the pointwise multiplication after it. So now let's get the fourier transform for a and the c .

$$a * \begin{pmatrix} 1 & 1 & 1 \\ 1 & e \frac{2\pi i}{3} & e \frac{\pi i}{3} \\ 1 & e \frac{\pi i}{3} & e \frac{2\pi i}{3} \end{pmatrix} = \begin{pmatrix} 2 & 1 + e \frac{\pi i}{3} & 1 + e \frac{2\pi i}{3} \end{pmatrix} \quad (35)$$

For c, it just is

$$(1 \quad 1 \quad 1) \quad (36)$$

Now, to get such a c, b after fourier transform must be

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{1 + e \frac{\pi i}{3}} & \frac{1}{1 + e \frac{2\pi i}{3}} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{1}{\sqrt{3}e \frac{\pi i}{6}} & \frac{1}{e \frac{\pi i}{3}} \end{pmatrix} \quad (37)$$

If we multiply this by the inverse fourier matrix we get

$$\frac{1}{3} \begin{pmatrix} \frac{1}{2} & \frac{1}{\sqrt{3}e \frac{\pi i}{6}} & \frac{1}{e \frac{\pi i}{3}} \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 1 & e \frac{\pi i}{3} & e \frac{2\pi i}{3} \\ 1 & e \frac{2\pi i}{3} & e \frac{\pi i}{3} \end{pmatrix} = \frac{1}{3} \begin{pmatrix} \frac{1}{2} + \frac{1}{\sqrt{3}e \frac{\pi i}{6}} + \frac{1}{e \frac{\pi i}{3}} \\ \frac{1}{2} + \frac{e \frac{\pi i}{6}}{\sqrt{3}} + e \frac{\pi i}{3} \\ \frac{1}{2} + \frac{e \frac{2\pi i}{3}}{\sqrt{3}} + 1 \end{pmatrix}^T \quad (38)$$

which might be a bit too chaotic.

ICE

1.

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} \quad (39)$$

2.

$x_0 + x_2 \quad x_0 - x_2 \quad x_1 + x_3 \quad x_1 - x_3$

3

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix} \quad (40)$$

is the same as

$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & i \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix} \quad (41)$$