1. I learned this from https://math.stackexchange.com/questions/3174003/dft-modulo-p-how-to-find-the-primitive-root-omega-n.

Thanks patrik. I'm not sure what p is but F_4 is

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 \\ 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^9 \end{pmatrix} \tag{1}$$

Now on Z_p, we are not dealing with complex numbers. We are dealing with integers. ω for Z_p at $p = 17$ is 7. Then, we want ω such that $\omega_4^4 = 7^{17-1} = 7^16$ so $\omega = 7^4 \mod p = 4$ so

$$F_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 4 & 16 & 13 \\ 1 & 16 & 1 & 16 \\ 1 & 13 & 16 & 4 \end{pmatrix} \tag{2}$$

2. Testing out cooley-turkey factorization. We want to get in the form

$$(F_2 \otimes I_2) T_2^4 (I_2 \otimes F_2) L_2^4 \tag{3}$$

Given we have

$$F_4 x = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 4 & 16 & 13 \\ 1 & 16 & 1 & 16 \\ 1 & 13 & 16 & 4 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix} \tag{4}$$

we get

$$\begin{pmatrix} x_0 + x_1 + x_2 + x_3 \\ x_0 + 4x_1 + 16x_2 + 13x_3 \\ x_0 + 16x_1 + x_2 + 16x_3 \\ x_0 + 13x_1 + 16x_2 + 4x_3 \end{pmatrix} \tag{5}$$

Now, this can be simplified as

$$t_0 = x_0 + x_2 \tag{6}$$
$$t_1 = x_0 + 16x_2 \tag{7}$$
$$t_2 = x_1 + x_3 \tag{8}$$
$$t_3 = 4x_1 + 13x_3 \tag{9}$$
$$t_4 = 16t_2 \tag{10}$$
$$t_5 = 16t_3 \tag{11}$$

Then, the sum can be written as

$$\begin{pmatrix} t_0 + t_2 \\ t_1 + t_3 \\ t_0 + t_4 \\ t_1 + t_5 \end{pmatrix} \tag{12}$$

Lowering the number of computations from 12 additions to 8 additoins.

This is the same as

$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 16 & 0 \\ 0 & 1 & 0 & 16 \end{pmatrix} \tag{13}$$

This is $(F_2 \otimes I_2)$ as

$$(F_2 \otimes I_2) = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 16 & 0 \\ 0 & 1 & 0 & 16 \end{pmatrix} \tag{14}$$

So in

$$(F_2 \otimes I_2) T_2^4 (I_2 \otimes F_2) L_2^4 \tag{15}$$

The rest of the terms are transforming from xs to ts.

xs and ts in a matrix relation is

$$\begin{pmatrix} t_0 \\ t_1 \\ t_2 \\ t_3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 16 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 4 & 0 & 13 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix} \tag{16}$$

If we group together even/odd indices,

$$\begin{pmatrix} t_0 \\ t_1 \\ t_2 \\ t_3 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 16 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 4 & 13 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix} \tag{17}$$

Now, as 4, 13 is just 1, 16 times 4,

$$\begin{pmatrix} t_0 \\ t_1 \\ t_2 \\ t_3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 16 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 16 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix} \tag{18}$$

For F_2, it's $\omega_2^2 = 7^{17-1} = 7^16$ so 16.

$$F_2 = \begin{pmatrix} 1 & 1 \\ 1 & 16 \end{pmatrix} \tag{19}$$

$$(I_2 \otimes F_2) = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 16 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 16 \end{pmatrix} \tag{20}$$

So we have our factorization! The final result is

$$F_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 4 & 16 & 13 \\ 1 & 16 & 1 & 16 \\ 1 & 13 & 16 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 16 & 0 \\ 0 & 1 & 0 & 16 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 16 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 16 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{21}$$

$$= (F_2 \otimes I_2) T_2^4 (I_2 \otimes F_2) L_2^4 \tag{22}$$

3a.

$$x = \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix} = x_0 e_0^4 + x_1 e_1^4 + x_2 e_2^4 + x_3 e_3^4 \tag{23}$$

3b. e_i^n just selects the ith column of the matrix it's multiplying. So, if for all i, $Ae_i^n = Be_i^n$ then they are identical as all their columns are identical.

3c. $e_i^m \otimes e_j^n$ is for every place e_i^m is 0, we have a 0 matrix but in the one place where e_i^m isn't 0, we have e_j^n. The final vector size is mn and the one is at $i * n + j$ so e_{in+j}^{mn}

3d.

$$(e_i^m \otimes e_j^n) \otimes e_k^o = e_{in+j}^{mn} \otimes e_k^o = e_{ino+jo+k}^{mno} \tag{24}$$

$$e_i^m \otimes (e_j^n \otimes e_k^o) = e_i^m \otimes e_{jo+k}^{no} = e_{ino+jo+k}^{mno} \tag{25}$$

Thus associativity holds true for here.

3e.

$$e_i^2 \otimes e_j^2 \otimes e_k^2 = e_{4i+2j+k}^8 \tag{26}$$

4.

$$L_n^{mn}(e_i^m \otimes e_j^n) = (e_j^n \otimes e_i^m) \tag{27}$$

This L_n^{mn} basically just changes the location of the one from idx $in + j$ to $jm + i$.

Since

$$e_{i_0}^2 \otimes ....e_{i_{k-1}}^2 = e_{2^k i_0 + 2^{k-1} i_1 .... i_{k-1}} \tag{28}$$

What R_{2^k} moves this to

$$e^2_{i_{k-1}} \otimes ....e^2_{i_0} = e_{2^k i_{k-1} + 2^{k-1} i_{k-2} .... i_0} \tag{29}$$

We can think of R_{2^k} as flipping a binary number.

So let's say we wanted to expand this. Let's say we want to calculate $R_{2^{k+1}}$. For this, one strategy we can use is flip the first k numbers in the binary representation. Then flip the final bit later. In practice we can think of this as $R_{2^k} \otimes R_{2^1}$ as for each bit in the original binary matrix expands by 2 by doing

$$e^2_{i_0} \otimes ....e^2_{i_{k-1}} \otimes e^2_{i_k} \tag{30}$$

Here, R_2 flips a bit. It's

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{31}$$

If we combine $R_2 \otimes R_2$ then we are flipping each bit individually and then we are flipping every 2 bits around. conceptually, if we keep flipping bits in this hierarchy way, we get a reverse binary. So

0010

to

0001

to

0100

So that's R_4. Can this be done in one step? Let's see

$$R_2 \otimes R_2 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \tag{32}$$

Basically, it's always the reverse of identity so i wonder if L is even needed?

5.

$$I_m \otimes \prod A_i = (I_m I_m .....) \otimes (A_0 A_1 ....) = (I_m \otimes A_0)(I_m \otimes A_1)..... = \prod (I_m \otimes A_i) \tag{33}$$

6a. F_n is symmetric as row i column j can be defined as ω^{ij} and same for column i row j.

6b.

$$L^{2m}_m (I_2 \otimes F_m) T^{2m}_m (F_2 \otimes I_m) \tag{34}$$

As

$$(L^{2m}_m)^T = L^{2m}_m \tag{35}$$

As it is symmetric. Same for F, T and I. As $F^T_n = F_n$, let's take the transpose of above

$$(F_2 \otimes I_m) T^{2m}_m (I_2 \otimes F_m) L^{2m}_m \tag{36}$$

cooley turkey says

$$F_n = (F_2 \otimes I_m) T_m^{2m} (I_2 \otimes F_m) L_m^{2m} \tag{37}$$

Next

$$F_{rs} = (F_r \otimes I_s) T_s^{rs} (I_r \otimes F_s) L_r^{rs} \tag{38}$$

$$T_s^{rs} = \begin{pmatrix} W_s^0 & 0 & 0 & .... \\ 0 & W_s^1 & 0 & .... \\ 0 & 0 & W_s^2 & .... \\ .. & .. & .. & ... \\ 0 & 0 & 0 & W_s^{r-1} \end{pmatrix} \tag{39}$$

Now where does

$$F_{2m} L_m^{2m} \tag{40}$$

come from?

From

$$\frac{C[x]}{X^{2m}-1} = f_0 + f_1 x + ... f_{2m-1} x^{2m-1} \tag{41}$$

to project down to

$$f(1), f(\omega) .... f(\omega^{2m-1}) \tag{42}$$

First stage factor $X^{2m} - 1$

$$X^{2m} - 1 = (X^m - 1)(X^m + 1) \tag{43}$$

$(X^m - 1)$ is all the even products of ω and the right is the odd powers.

For F_4, if $x^2 = 1(X^m - 1)$

$$f_0 + f_1 x + f_2 x^2 + f_3 x^3 = (f_0 + f_2) + (f_1 + f_3) x \tag{44}$$

if $x^2 = -1(X^m + 1)$

$$f_0 + f_1 x + f_2 x^2 + f_3 x^3 = (f_0 + f_2) - (f_1 + f_3) x \tag{45}$$

$$\frac{C[x]}{X^{2m}-1} = \frac{C[x]}{X^m - 1} X \frac{C[x]}{X^m + 1} \tag{46}$$

This is just? Replace X with ωX for the second one

$$F_m, W^m F_m \tag{47}$$

We do

$$F_{2m} = L_m^{2m} (I_2 \otimes F_m) T_m^{2m} (F_2 \otimes I_m) \tag{48}$$