

For simplicity, let $n = q - 1$.

Observe that, when $k \neq 0$,

$$\sum_{i=0}^{n-1} \alpha^{ik} = 0, \forall \alpha \in \mathbb{Z}_q^*,$$

and when $k = 0$, obviously

$$\sum_{i=0}^{n-1} \alpha^{ik} = \sum_{i=0}^{n-1} \alpha^0 = n, \forall \alpha \in \mathbb{Z}_q^*.$$

Therefore we have

$$\begin{aligned} f(i) &= \frac{1}{n} \sum_{k,j} f(j) \alpha^{k(j-i)} \\ &= \frac{1}{n} \sum_{k,j} f(j) \alpha^{kj-ki} \\ &= \frac{1}{n} \sum_{k,j} f(j) \alpha^{kj} \alpha^{-ik}. \end{aligned}$$

Let $F(k) \stackrel{\text{def}}{=} \sum_j f(j) \alpha^{kj}$, then

$$f(i) = \frac{1}{n} \sum_k F(k) \alpha^{-ik}.$$

We can compute $F(k)$ recursively —

$$\begin{aligned} F(k) &= \sum_{j=0}^{n-1} f(j) \alpha^{kj} \\ &= \sum_{l=0}^{n/2-1} f(2l) \alpha^{k \cdot 2l} + \alpha^k \sum_{l=0}^{n/2-1} f(2l+1) \alpha^{k \cdot 2l} \\ &= G(k') + \alpha^k H(k'), \end{aligned}$$

where G and H are the NTT's of functions relevant to f , and $k' \stackrel{\text{def}}{=} k \bmod n/2$, and will be just denoted k from now on.