Source task and conventions

For $n = 2^k \geq 2$, $m = 2^{tn/2} + 1$ and $\omega = 2^t \pmod{m}$, prove that the DFT and inverse are well defined even when m is composite.

Conventional solution and proof

The modulus is odd, so both two and n are units modulo m. Also $\omega^{n/2} = 2^{tn/2} = -1 \pmod{m}$, giving $\omega^n = 1$. Its order is exactly n: every proper divisor of the power-of-two n divides $n/2$, where the value is not one. The essential point is orthogonality without division by a possible zero divisor. For $0 < r < n$, write $r = 2^s u$ with odd u and $0 \leq s < k$. Put $L = n/2^s$. In each block of L terms of $\sum_{j=0}^{n-1} \omega^{rj}$, pair index j with $j + L/2$. The ratio is $\omega^{rL/2} = \omega^{un/2} = (-1)^u = -1$. Every pair cancels, so the sum is zero modulo m. For $r = 0$ the sum is n. Define $V_{kj} = \omega^{kj}$ and $W_{jk} = n^{-1}\omega^{-jk}$. The preceding sums give $(WV)_{jl} = \delta_{jl}$ and likewise $VW = I$. Thus both transforms are well-defined inverse linear maps over $\mathbb{Z}/m\mathbb{Z}$.

Structural or analytic derivation

This is a principal-root construction in a ring, not an argument that the ring is a field. The pair-cancellation proof supplies the exact property needed by the butterfly recursion. The usual geometric-series step dividing by $1 - \omega^r$ would be unjustified when that element is a zero divisor.

Comparative cost and preferred method

The radix-two algorithm uses $O(n \log n)$ ring operations and avoids floating roundoff. However m has $tn/2 + 1$ bits, so a ring operation is not a constant-cost machine-word operation as n grows. The next source problem supplies an alternative prime-modulus word model. The one-point DFT is trivially the identity; the printed modulus formula needs separate interpretation at $n = 1$ when $tn/2$ is nonintegral.