Source task and conventions

For two n-element sets of integers in $[0, 10n]$, compute all sum multiplicities in $O(n \log n)$ arithmetic.

Conventional solution and proof

Create indicator polynomials $A(z) = \sum_{a \in \mathcal{A}} z^a$ and $B(z) = \sum_{b \in \mathcal{B}} z^b$. Their product has coefficient

$$c_k = [z^k]A(z)B(z) = \#\{(a, b) \in \mathcal{A} \times \mathcal{B} : a + b = k\}.$$

This follows by distributing the finite sums; each ordered pair contributes one monomial. Form the product by a length-M convolution with $M \geq 20n + 1$ chosen as a suitable FFT length. Read the coefficients with $c_k > 0$ to obtain the Cartesian-sum set, and retain c_k as its multiplicity. Building the indicators and scanning the output cost $O(n)$; the transform product costs $O(n \log n)$ in the source's arithmetic model.

Structural or analytic derivation

For exact integer output, a number-theoretic transform with a supported primitive Mth root can replace complex floating arithmetic. Since the inputs are sets, every coefficient is at most n: for each a, at most one $b = k - a$ contributes. A prime modulus $p > n$ therefore determines the nonnegative coefficient uniquely, provided it supports the chosen transform. More generally CRT reconstruction requires a combined modulus exceeding a proved coefficient bound. A floating FFT needs an error enclosure below $1/2$ before rounding can be certified.