Source task and conventions

Solve the heuristic prime-search, invertibility, FFT implementation and explicit modulus-17 calculation in CLRS Problem 30-5.

Conventional solution and proof

(a) Near $p = kn + 1$, prime-density heuristics assign probability on the order of $1/\log p$ to a candidate (with a constant adjustment for the fixed odd progression when $n \geq 2$ is a power of two). This suggests $\Theta(\log n)$ trials and a typical p of order $n \log n$. Its bit length is $\log_2 n + O(\log\log n) = \Theta(\log n)$. This is the requested heuristic, not a proved expectation for the first prime in this progression. (b) A generator g of the multiplicative group modulo p has order kn. Thus $w = g^k$ has order n. For $0 < r < n$, $1 - w^r \neq 0$ is invertible in the field, and the geometric sum $\sum_{j=0}^{n-1} w^{rj} = 0$. Also n is nonzero modulo p. These facts prove that $n^{-1}w^{-jk}$ is the inverse DFT matrix. (c) Apply the radix-two recursion with all additions and multiplications reduced modulo p. The combine identity is polynomial algebra and remains valid in this field. Use w^{-1} and one final multiplication by n^{-1} for the inverse. The recurrence $T(n) = 2T(n/2) + \Theta(n)$ gives $\Theta(n \log n)$ operations on the stipulated $O(\log n)$-bit words. (d) Modulo 17, $3^4 = 13$, $3^8 = 16 = -1$ and $3^{16} = 1$, so three has order 16. For $n = 8$, take $w = 3^2 = 9$ and $8^{-1} = 15$. The full transform of $(0, 5, 3, 7, 7, 2, 1, 6)$ is printed in the executable-results table; each entry is calculated by $\sum_{j=0}^{7} a_j 9^{jk} \pmod{17}$, and the inverse is checked exactly.

Structural or analytic derivation

Finite-field orthogonality gives an exact analogue of the complex Fourier basis. Integer convolution is recovered from modular coefficients only after a coefficient bound is supplied: one modulus does not distinguish arbitrary integers congruent modulo p. CRT or a sufficiently large prime provides the additional information.

Comparative cost and preferred method