graphic notes and further reading. 2. Computational/algorithmic number theory. 2.1. Introduction. 2.1.1. What is computational/algorithmic number theory? 2.1.2. Effective computability. 2.1.3. Computational complexity. 2.1.4. Complexity of number-theoretic algorithms. 2.1.5. Fast modular exponentations. 2.1.6. Fast group operations on elliptic curves. 2.2. Algorithms for primality testing. 2.2.1. Deterministic and rigorous primality tests. 2.2.2. Fermat's pseudoprimality test. 2.2.3. Strong psuedoprimality test. 2.2.4. Lucas pseudoprimality test. 2.2.5. Elliptic curve test. 2.2.6. Historical notes on primality testing. 2.3. Algorithms for integer factorization. 2.3.1. Complexity of integer factorization. 2.3.2. Trial division and Fermat method. 2.3.3. Legendre's congruence. 2.3.4. Continued FRACtion method (CFRAC). 2.3.5. Quadratic and number field sieves (QS/NFS). 2.3.6. Polland's "*rho*" and "$p-1$" methods. 2.3.7. Lenstra's elliptic curve method (ECM). 2.4. Algorithms for discrete logarithms. 2.4.1. Shanks' baby-step giant step-algorithm. 2.4.2. Silver-Pohlig-Hellman algorithm. 2.4.3. Index calculus for discrete logarithms. 2.4.4. Algorithms for elliptic curve discrete logarithms. 2.4.5. Algorithm for root finding problem. 2.5. Quantum number-theoretic algorithms. 2.5.1. Quantum information and computation. 2.5.2. Quantum computability and complexity. 2.5.3. Quantum algorithm for integer factorization. 2.5.4. Quantum algorithms for discrete logarithms. 2.6. Miscellaneous algorithms in number theory. 2.6.1. Algorithms for computing $\pi(x)$. 2.6.2. Algorithms for generating amicable pairs. 2.6.3. Algorithms for verifying Goldbach's conjecture. 2.6.4. Algorithm for finding odd perfect numbers. 2.7. Bibliographic notes and further reading. 3. Applied number theory in computing/cryptography. 3.1. Why applied number theory? 3.2. Computer systems design. 3.2.1. Representing numbers in residue number systems. 3.2.2. Fast computations in residue number systems. 3.2.3. Residue computers. 3.2.4. Complementary arithmetic. 3.2.5. Hash functions. 3.2.6. Error detection and correction methods. 3.2.7. Random number generation. 3.3. Cryptography and information security. 3.3.1. Introduction. 3.3.2. Secret-key cryptography. 3.3.3. Data/advanced encryption standard (DES/AES). 3.3.4. Public-key cryptography. 3.3.5. Discrete logarithm based cryptosystems. 3.3.6. RSA public-key cryptosystem. 3.3.7. Quadratic residuosity cryptosystems. 3.3.8. Elliptic curve public-key cryptosystems. 3.3.9. Digital signatures. 3.3.10. Digital signature standard (DSS). 3.3.11. Database security. 3.3.12. Secret sharing. 3.3.13. Internet/web security and electronic commerce. 3.3.14. Steganography. 3.3.15. Quantum cryptography. 3.4. Bibliographic notes and further reading. Bibliography. Index.

Tabular Application Development for Information Systems: An Object-Oriented Methodology. By Talib Damij. Springer, New York. (2001). 190 pages. $54.95. (CD-Rom included.)
Contents:

Preface. Acknowledgments. I. Introduction. 1. Overview. 2. Object-oriented concepts. 2.1. Objects. 2.2. Classes. 2.3. Attributes. 2.4. Associations. 2.5. Operations. 2.6. Inheritance. 3. Methodology preview. II. Methodology. 4. Problem definition. 4.1. Tourist organization. 5. Systems functioning. 5.1. Activities. 5.1.1. Activity table development. 5.1.2. Tourist organization. 5.2. Tasks. 5.2.1. Task table development. 5.2.2. Tourist organization. 5.3. Work processes and business processes. 5.3.1. Tourist organization. 6. Business process reengineering. 6.1. Table analysis and reengineering. 6.1.1. Tourist organization. 6.2. Process model. 6.2.1. Tourist organization. 7. Object mall. 7.1. Semantic network modeling. 7.2. Functional dependence. 7.3. Object model development. 7.3.1. Tourist organization. 8. Design. 8.1. Operations. 8.1.1. Tourist organization. 8.2. Application model. 8.2.1. Tourist organization. 9. Implementation. III. Applications. 10. Internal clinic. 10.1. Problem definition. 10.2. Systems functioning. 10.2.1. Activity table development. 10.2.2. Task table development. 10.2.3. Work processes and business processes. 10.3. Business process reengineering. 10.3.1. Table analysis and reengineering. 10.3.2. Process model. 10.4. Object model. 10.5. Design. 10.5.1. Operations. 10.5.2. Application model. 11. Clinic for small animals. 11.1. Problem definition. 11.2. Systems functioning. 11.2.1. Activity table development. 11.2.2. Task table development. 11.2.3. Work processes and business processes. 11.3. Business process reengineering. 11.3.1. Table analysis and reengineering. 11.3.2. Process model. 11.4. Object model. 11.5. Design. 11.5.1. Operations. 11.5.2. Application model. 12. Payment movement. 12.1. Problem definition. 12.2. Systems functioning. 12.2.1. Activity table development. 12.2.2. Task table development. 12.2.3. Work processes and business processes. 12.3. Business process reengineering. 12.3.1. Process model. 12.4. Object model. 12.5. Desing. 12.5.1. Operations. 12.5.2. Application model. 13. Student office. 13.1. Problem definition. 13.2. Systems functioning. 13.2.1. Activity table development. 13.2.2. Task table development. 13.2.3. Work processes and business processes. 13.3. Business process reengineering. 13.3.1. Process model. 13.4. Object model. 13.5. Design. 13.5.1. Operations. 13.5.2. Application model. IV. TAD case-tool. 14. TAD case-tool. 14.1. Installation and start. 14.2. Application. 14.2.1. Creating an application. 14.2.2. Opening an application. 14.3. TAD main menu. 14.4. Entity table. 14.4.1. New entity. 14.4.2. Entity properties. 14.4.3. Delete entity. 14.4.4. New analysis. 14.4.5. Analysis properties. 14.4.6. Delete analysis. 14.4.7. Linkage definition. 14.4.8. Sorting analyses. 14.4.9. Changing position and refreshing. 14.5. Activity table. 14.5.1. Entity. 14.5.2. Activity. 14.5.3. Horizontal linkage. 14.5.4. Vertical linkage. 14.6. Task table. 14.7. Work processes. 14.8. Business processes. 14.9. Application model. References. Index.

Computational Methods for Fluid Dynamics. Third Edition. By J. H. Ferziger. and M. Perić. Springer, New York. (2002). 423 pages. $54.95.
Contents:

Preface. 1. Basic concepts of fluid flow. 1.1. Introduction. 1.2. Conservation principles. 1.3. Mass conservation. 1.4. Momentum conservation. 1.5. Conservation of scalar quantities. 1.6. Dimensionless form of equations. 1.7. Simplified mathematical models. 1.7.1. Incompressible flow. 1.7.2. Inviscid (Euler) flow. 1.7.3. Potential flow.

1.7.4. Creeping (Stokes) flow. 1.7.5. Boussinesq approximation. 1.7.6. Boundary layer approximation. 1.7.7. Modeling of complex flow phenomena. 1.8. Mathematical classification of flows. 1.8.1. Hyperbolic flows. 1.8.2. Parabolic flows. 1.8.3. Elliptic flows. 1.8.4. Mixed flow types. 1.9. Plan of this book. 2. Introduction to numerical methods. 2.1. Approaches to fluid dynamical problems. 2.2. What is CFD? 2.3. Possibilities and limitations of numerical methods. 2.4. Components of a numerical solution method. 2.4.1. Mathematical model. 2.4.2. Discretization method. 2.4.3. Coordinate and basis vector systems. 2.4.4. Numerical grid. 2.4.5. Finite approximations. 2.4.6. Solution method. 2.4.7. Convergence criteria. 2.5. Properties of numerical solution methods. 2.5.1. Consistency. 2.5.2. Stability. 2.5.3. Convergence. 2.5.4. Conservation. 2.5.5. Boundedness. 2.5.6. Realizability. 2.5.7. Accuracy. 2.6. Discretization approaches. 2.6.1. Finite difference method. 2.6.2. Finite volume method. 2.6.3. Finite element method. 3. Finite difference methods. 3.1. Introduction. 3.2. Basic concept. 3.3. Approximation of the first derivative. 3.3.1. Taylor series expansion. 3.3.2. Polynomial fitting. 3.3.3. Compact schemes. 3.3.4. Non-uniform grids. 3.4. Approximation of the second derivative. 3.5. Approximation of mixed derivatives. 3.6. Approximation of other terms. 3.7. Implementation of boundary conditions. 3.8. The algebraic equation system. 3.9. Discretization errors. 3.10. An introduction to spectral methods. 3.10.1. Basic concept. 3.10.2. Another view of discretization error. 3.11. Example. 4. Finite volume methods. 4.1. Introduction. 4.2. Approximation of surface integrals. 4.3. Approximation of volume integrals. 4.4. Interpolation and differentiation practices. 4.4.1. Upwind interpolation (UDS). 4.4.2. Linear interpolation (CDS). 4.4.3. Quadratic upwind interpolation (QUICK). 4.4.4. Higher-order schemes. 4.4.5. Implementation of boundary conditions. 4.6. The algebraic equation system. 4.7. Examples. 5. Solution of linear equation system. 5.1. Introduction. 5.2. Direct methods. 5.2.1. Gauss elimination. 5.2.2. LU decomposition. 5.2.3. Tridiagonal systems. 5.2.4. Cyclic reduction. 5.3. Iterative methods. 5.3.1. Basic concept. 5.3.2. Convergence. 5.3.3. Some basic methods. 5.3.4. Incomplete LU decomposition: Stone's method. 5.3.5. ADI and other splitting methods. 5.3.6. Conjugate gradient methods. 5.3.7. Biconjugate gradients and CGSTAB. 5.3.8. Multigrid methods. 5.3.9. Other iterative solvers. 5.4. Coupled equations and their solution. 5.4.1. Simultaneous solution. 5.4.2. Sequential solution. 5.4.3. Under-relaxation. 5.5. Non-linear equations and their solution. 5.5.1. Newton-like techniques. 5.5.2. Other techniques. 5.6. Deferred-correction approaches. 5.7. Convergence criteria and iteration errors. 5.8. Examples. 6. Methods for unsteady problems. 6.1. Introduction. 6.2. Methods for initial value problems in ODEs. 6.2.1. Two-level methods. 6.2.2. Predictor-corrector and multipoint methods. 6.2.3. Runge-Kutta methods. 6.2.4. Other methods. 6.3. Application to the generic transport equation. 6.3.1. Explicit methods. 6.3.2. Implicit methods. 6.3.3. Other methods. 6.4. Examples. 7. Solution of the Navier-Stokes equations. 7.1. Special features of the Navier-Stokes equations. 7.1.1. Discretization of convective and viscous terms. 7.1.2. Discretization of pressure terms and body forces. 7.1.3. Conservation properties. 7.2. Choice of variable arrangement on the grid. 7.2.1. Colocated arrangement. 7.2.2. Staggered arrangements. 7.3. Calculation of the pressure. 7.3.1. The pressure equation and its solution. 7.3.2. A simple explicit time advance scheme. 7.3.3. A simple implicit time advance method. 7.3.4. Implicit pressure-correction methods. 7.4. Other methods. 7.4.1. Fractional step methods. 7.4.2. Streamfunction-vorticity methods. 7.4.3. Artificial compressibility methods. 7.5. Solution methods for the Navier-Stokes equations. 7.5.1. Implicit scheme using pressure-correction and staggered grid. 7.5.2. Treatment of pressure for colocated variables. 7.5.3. SIMPLE algorithm for a colocated variable arrangement. 7.6. Note on pressure and incompressibility. 7.7. Boundary conditions for the Navier-STokes equations. 7.8. Examples. 8. Complex geometries. 8.1. The choice of grid. 8.1.1. Stepwise approximation using regular grids. 8.1.2. Overlapping grids. 8.1.3. Boundary-fitted non-orthogonal grids. 8.2. Grid generation. 8.3. The choice of velocity components. 8.3.1. Grid-oriented velocity components. 8.3.2. Cartesian velocity components. 8.4. The choice of variable arrangement. 8.4.1. Staggered arrangements. 8.4.2. Colocated arrangement. 8.5. Finite difference methods. 8.5.1. Methods based on coordinate transformation. 8.5.2. Method based on shape functions. 8.6. Finite volume methods. 8.6.1. Approximation of convective fluxes. 8.6.2. Approximation of diffusive fluxes. 8.6.3. Approximation of source terms. 8.6.4. Three-dimensional grids. 8.6.5. Block-structured grids. 8.6.6. Unstructured grids. 8.7. Control-volume-based finite element methods. 8.8. Pressure-correction equation. 8.9. Axi-symmetric problems. 8.10. Implementation of boundary conditions. 8.10.1. Inlet. 8.10.2. Outlet. 8.10.3. Impermeable walls. 8.10.4. Symmetry planes. 8.10.5. Specified pressure. 8.11. Examples. 9. Turbulent flows. 9.1. Introduction. 9.2. Direct numerical simulation (DNS). 9.2.1. Example: Spatial decay of grid turbulence. 9.3. Large eddy simulation (LES). 9.3.1. Smagorinsky and related methods. 9.3.2. Dynamic models. 9.3.3. Deconvolution models. 9.3.4. Example: Flow over a wall-mounted cube. 9.3.5. Example: Stratified homogeneous shear flow. 9.4. RANS models. 9.4.1. Reynolds-averaged Navier-Stokes (RANS) equations. 9.4.2. Simple turbulence models and their application. 9.4.3. The v2f model. 9.4.4. Example: Flow around an engine valve. 9.5. Reynolds stress models. 9.6. Very large eddy simulation. 10. Compressible flows. 10.1. Introduction. 10.2. Pressure-correction methods for arbitrary mach number. 10.2.1. Pressure-velocity-density coupling. 10.2.2. Boundary conditions. 10.2.3. Examples. 10.3. Methods designed for compressible flow. 10.3.1. An overview of some specific methods. 11. Efficiency and accuracy improvement. 11.1. Error analysis and accuracy improvement. 11.1. Error analysis and estimation. 11.1.1. Description of errors. 11.1.2. Estimation of errors. 11.1.3. Recommended practice for CFD uncertainty analysis. 11.2. Grid quality and optimization. 11.3. Multigrid methods for flow calculation. 11.4. Adaptive grid methods and local grid refinement. 11.5. Parallel computing in CFD. 11.5.1. Iterative schemes for linear equations. 11.5.2. Domain decomposition in space. 11.5.3. Domain decomposition in time. 11.5.4. Efficiency of parallel computing. 12. Special topics. 12.1. Introduction. 12.2. Heat and mass transfer. 12.3. Flows with variable fluid properties. 12.4. Moving grids. 12.5. Free-surface flows. 12.5.1. Interface-tracking methods. 12.5.2. Hybrid methods. 12.6. Meteorological and oceanographic applications. 12.7. Meteorological and oceanographic applications. 12.7. Multiphase flows. 12.8. Conclusions. A. Appendices. A.1. List of computer codes and how to access them. A.2. List of frequently used abbreviations. References. Index.