ally closed, real closed and the rational p-adic fields. Local fields (Preparatory results. The equal characteristic case. The unequal characteristic case). Extensions of algebraic number fields. Brandis' theorem. Fields with free multiplicative groups modulo torsion. A nonsplitting example. Embedding groups. Multiplicative groups under field extensions.

Neal Koblitz, A Course in Number Theory and Cryptography (Springer, New York, 1987) 208 pages

Chapter I: *Some Topics in Elementary Number Theory.* Time estimates for doing arithmetic. Divisibility and the Euclidean algorithm. Congruences. Some applications to factoring. *Chapter* II: *Finite Fields and Quadratic Residues.* Finite fields. Quadratic residues and reciprocity. *Chapter* III: *Cryptography.* Some simple cryptosystems. Enciphering matrices. *Chapter* IV: *Public Key.* The idea of public key cryptography. RSA. Discrete log. Knapsack. *Chapter* V: *Primality and Factoring.* Pseudoprimes. The rho method. Fermat factorization and factor bases. The continued fraction method. *Chapter* VI: *Elliptic Curves.* Basic facts. Elliptic curve cryptosystems. Elliptic curve factorization.

Emile Aarts and Jan Korst, Simulated Annealing and Boltzmann Machines: A Stochastic Approach to Combinatorial Optimization and Neural Computing (Wiley, Chichester, 1989) 272 pages

I: Simulated Annealing. 1: *Combinatorial Optimization.* Combinatorial optimization problems. Local search. 2: *Simulated Annealing.* The Metropolis algorithm. The simulated annealing algorithm. Equilibrium statistics. Characteristic features. A quantitative analysis. 3: *Asymptotic Convergence.* Markov theory. The stationary distribution. Inhomogeneous Markov chains. Convergence in distribution. Asymptotic behaviour. 4: *Finite-Time Approximation.* Cooling schedules. A polynomial-time cooling schedule. Empirical performance analysis. 5: *Simulated Annealing in Practice.* Implementing the algorithm (The travelling salesman problem. The max cut problem. The independent set problem. The graph colouring problem. The placement problem). A survey of applications (Basic problems. Engineering problems). General performance experiences. 6: *Parallel Simulated Annealing Algorithms.* Speeding up the simulated annealing algorithm. Parallel-machine models. Designing parallel annealing algorithms. General algorithms (The division algorithm. The clustering algorithm. The error algorithm. Parallel implementation and numerical results). II: Boltzmann Machines. 7: *Neural Computing.* Man versus machine. Connectionist models. A historical overview. The Boltzmann machine. 8: *Boltzmann Machines.* Structural description. Sequential Boltzmann machines. Parallel Boltzmann machines (Synchronous parallelism. Asynchronous parallelism. A parallel cooling schedule). A taxonomy. 9: *Combinatorial Optimization and Boltzmann Machines.* General strategy. The max cut problem. The independent set problem. The graph colouring problem. The clique partitioning and clique covering problems. The travelling salesman problem. Numerical results (Graph problems. The travelling salesman problem). 10: *Classification and Boltzmann Machines.* Classification problems. Extension of the structural description. Examples (Classification without hidden units. Classification with hidden units. Association. Fault tolerance). 11: *Learning and Boltzmann Machines.* Learning from examples. Equilibrium properties. Learning without hidden units (Outline of the learning algorithm. Estimation of activation probabilities). Learning with hidden units. Variants of the learning algorithm. Learning in practice (Choosing a desired visible behaviour. Convergence properties. Estimation of the activation probabilities. Termination of the learning algorithm). Robustness aspects (Internal representations. Relearning).