POLYNOMIALS IN COMPUTER ALGEBRA

by Maurice Mignotte, Strasbourg

In this series of lectures we shall study algorithms on polynomials which are of great importance in Computer Algebra. The different situations which are considered are polynomials over general rings (gcd computation, chinese theorem and interpolation, resultants, squarefree factorization, ...), polynomials over complex numbers (estimates for the roots, bounds for the factors, separation of the roots, ...), polynomials with real coefficients (estimates for the real roots, separation of the real roots, rules of Descartes, Newton, Budan-Fourier, Sturm method, ...), polynomials over finite fields (algorithms in finite fields, factorization of polynomials, statistical studies, ...) and the final chapter deals with polynomials with integer cooefficients (Hensel lifting, factorization in the past and modern methods, LLL algorithm, ...).

The presentation will always be as constructive and algorithmic as possible. We present concrete experiences with systems of computer algebra (mainly PARI) and study the cost of the different algorithms. There is some emphasis on problems which occur simultaneouly in Diophantine Approximation and in Computer Algebra. We also discuss some open problems.