

# Mathematics and Algorithms for Computer Algebra

Dr Francis J. Wright & Dr James E. F. Skea

July 9, 2003

The intention of this course is to recapitulate basic mathematical structures from a constructive and algorithmic viewpoint, and then present some of the fundamental algorithms on these structures that underlie computer algebra. It will be primarily a theoretical course that is not tied to any particular computer algebra system, although we may occasionally refer to Maple, REDUCE and Derive for examples of actual implementations. It is proposed to consist of about 28 2-hour lectures, together with typeset lecture notes.

The following syllabus shows in broad outline the material that we intend to cover, but we reserve the right to vary the details. The course language will be English, which we will attempt to speak slowly, and there will be people who can translate.

## **Part 1: Dr Francis J. Wright.**

### **1 Introduction to computing aspects**

- Data types and tasks of CA
- The main CA systems: Maple, REDUCE, Derive, etc.
- Data representations and their implementation
- Normal and canonical representations
- Data ordering – lexicographic, total degree, etc.
- Introduction to complexity of algorithms

### **2 Introduction to algebraic aspects**

- Revision (?) of basic notions
- Mathematical structures for CA: groups, rings, integral domains

and fields, and the arithmetic operations defined on them

### **3 Integer and rational arithmetic**

Representation of integers  
Integer arithmetic; Euclidean division  
Complexity  
Computation of powers  
GCD; prime numbers  
Rational arithmetic (an application of gcds)

### **4 Polynomial algebra**

Definitions  
Arithmetic and simplification; rational functions  
Euclidean division; pseudo-division  
Irreducibility; content  
Polynomial functions; roots of polynomials  
The resultant

### **5 Polynomial GCDs and remainder sequences**

Square-free factorization – an application of gcds  
Computation of gcds in terms of content and primitive part  
Pseudo-remainder sequences: Euclidean, primitive and subresultant  
The subresultant theorem  
Bézout's identity; partial fraction decomposition

### **6 Univariate polynomial equations**

Sturm sequences  
Root bounds  
Possibly other topics, such as polynomial decomposition, Akritas' root-isolation method

## **7 Introduction to modular and $p$ -adic methods**

- Homomorphic images
- Chinese remainder theorem for integers
- Polynomials over finite fields
- Modular integer GCD computations
- The  $p$ -adic numbers
- Newton's iteration; Hensel lifting

### **Part 2: Dr Jim E. F. Skea.**

## **8 Univariate Polynomials**

### **8.1 Algorithms for performing GCD**

- Good and bad reductions
- Euclid's Algorithm for Modular Polynomials
- Hensel Lifting
- The Landau-Mignotte Bound
- Gelfand's Bound

### **8.2 Factorisation**

- The Chinese Remainder Theorem for Polynomials
- The Frobenius Map
- Berlekamp's Method
- Cyclotomic Polynomials

## **9 Multivariate Polynomials**

- Kronecker's Method
- Wang's Method
- Image Sets
- EEZ-lifting

## **10 Gröbner Bases**

- Buchberger's Algorithm
- Solving Systems of Nonlinear Polynomial Equations

## 11 Symbolic Integration

Differential Fields  
Elementary Extensions  
Liouville's Theorem  
Risch's Algorithm  
The Risch-Norman Method  
The Trager-Rothstein Method  
The Fitch "Superbound"

### Books

The course will be based mainly on the following texts, among which those by Mignotte and Davenport et al. are probably the most important:-

- Mignotte, M. (1992). *Mathematics for Computer Algebra*. Springer-Verlag, New York
- Lipson, J. D. (1981). *Elements of algebra and algebraic computing*. Addison-Wesley, Redwood City, California
- Akritas, A. G. (1989). *Elements of computer algebra with applications*. Wiley-Interscience, New York

for the mathematical background and fundamental algorithms, and

- Davenport, J. H., Siret, Y., and Tournier, E. (1988). *Computer algebra: systems and algorithms for algebraic computation*. Academic Press, London
- Buchberger, B., Collins, G. E., Loos, R., with Albrecht, R. (eds.) (1983). *Computer algebra: symbolic and algebraic computation*. (2nd edn). Springer-Verlag, Wien

for the computational aspects and remaining algorithmic content.