

## Computer Algebra (C001026)

**Course size** *(nominal values; actual values may depend on programme)*

**Credits 6.0**

**Study time 165 h**

**Course offerings and teaching methods in academic year 2025-2026**

A (semester 2)

Dutch

Gent

seminar  
lecture

**Lecturers in academic year 2025-2026**

Weiermann, Andreas

WE16

lecturer-in-charge

De Beule, Jan

VUB

co-lecturer

**Offered in the following programmes in 2025-2026**

[Master of Science in Teaching in Science and Technology\(main subject Mathematics\)](#)

**crdts**

6

**offering**

A

[Master of Science in Computer Science](#)

6

A

[Master of Science in Mathematics](#)

6

A

**Teaching languages**

Dutch

**Keywords**

Fast multiplication, modular algorithms, greatest common divisor, primality testing, algebra of polynomials, factorization of integers and polynomials, Gröbner bases

**Position of the course**

This course is an introduction to a field that one can describe as "computer algebra". This course is exclusively devoted to algorithms for exact computations. These algorithms fit in with the algebraic knowledge of the bachelor programme. The main goal is twofold. The students have to study these algorithms and they have to design algorithms for certain problems using their theoretical knowledge.

**Contents**

Typical algorithms are studied in this course. After an introduction to the field and the discussing of technical aspects such as representation of data, we study algorithms that can be classified as follows.

- 1 Fundamental algorithms: representation of integers and polynomials, addition of integers and polynomials. Classical algorithms for multiplications, division, and exponentiation. Euclid's extended algorithm for the greatest common divisor and applications. Chinese remainder theorem.
- 2 Faster algorithms for multiplication: the algorithm of Karatsuba, Fast Fourier transform, and the algorithm of Schönhage and Strassen. Division with remainder using Newton iteration.
- 3 Algorithms for the greatest common divisor: gcd of polynomials over a Unique Factorisation Domain. Modular algorithms for the gcd in a UFD: a big prime algorithm for the gcd in  $F[X,Y]$ ,  $F$  a field and  $Z[X]$ . A small prime algorithm for  $Z[X]$ .
- 4 Primality testing and integer factorization: Pollard's rho-method, the quadratic sieve; application: RSA.
- 5 Factorisation of polynomials: squarefree factorisation, factorisation over finite fields. A big prime algorithm for factorisation in  $Z[X]$ , Hensel lifting and Zassenhaus' algorithm for factorization in  $Z[X]$ . If time permits: the LLL basis reduction algorithm with an more efficient algorithm for factorization over  $Z[x]$  as an application.

6 Gröbner bases for polynomial ideals, and applications: e.g. automatic proof generating.

### **Initial competences**

Basic knowledge of algebra (polynomial rings, ideals, finite fields) and programming. For bachelors of mathematics: the courses "Algebra I" and "Practicum Wiskunde" contain the prerequisites. For bachelors of informatics: the courses "Lineaire algebra en meetkunde", "Discrete wiskunde" and "Programmeren I" contain the prerequisites.

### **Final competences**

- 1 Being able to explain algorithms from the course.
- 2 Being able to analyse algebraic knowledge and to translate it to algorithms.
- 3 Being able to evaluate with critical sense results obtained by using computer algebra systems.

### **Conditions for credit contract**

Access to this course unit via a credit contract is determined after successful competences assessment

### **Conditions for exam contract**

This course unit cannot be taken via an exam contract

### **Teaching methods**

Seminar, Lecture

### **Extra information on the teaching methods**

A complete set of lecture notes inclusive a package with exercises is available.

### **Study material**

Type: Syllabus

Name: Computeralgebra

Indicative price: Free or paid by faculty

Optional: no

Language : Dutch

Number of Pages : 203

Available on Ufora : Yes

Online Available : Yes

Available in the Library : No

Available through Student Association : No

### **References**

J. von zur Gathen and J. Gerhard, "Modern computer algebra", Cambridge University Press, Cambridge, third edition, 2013. (ISBN: 9781107039032)

### **Course content-related study coaching**

During the lectures, the algorithms are explained in detail. During the exercise classes the algorithms are illustrated.

### **Assessment moments**

end-of-term and continuous assessment

### **Examination methods in case of periodic assessment during the first examination period**

Oral assessment

### **Examination methods in case of periodic assessment during the second examination period**

Oral assessment

### **Examination methods in case of permanent assessment**

Assignment

### **Possibilities of retake in case of permanent assessment**

examination during the second examination period is possible

### **Extra information on the examination methods**

Periodical evaluation: examination is written (closed book)

Non-periodical evaluation: presentation and project.

### **Calculation of the examination mark**

Periodical evaluation (50%) + non-periodical evaluation (50%).

In case the student fails for this course, he can get a second chance to make a

(Approved)

similar project for the non-periodical evaluation.