UNIVERSITEIT GENT

Studiefiche

Vanaf academiejaar 2024-2025

Computeralgebra (C001026)

Cursusomvang *(nominale waarden; effectieve waarden kunnen verschillen per opleiding)*

Studiepunten 6.0 **Studietijd 165 u**

Aanbodsessies en werkvormen in academiejaar 2024-2025

A (semester 2)	Nederlands	Gent	hoorcollege
			werkcollege

Lesgevers in academiejaar 2024-2025

Weiermann, Andreas	WE16	Verantwoordelijk lesgever
De Beule, Jan	VUB	Medelesgever

Aangeboden in onderstaande opleidingen in 2024-2025	**stptn**	**aanbodsessie**
Educatieve Master of Science in de wetenschappen en technologie(afstudeerrichting wiskunde)	6	A
Master of Science in de informatica	6	A
Master of Science in de wiskunde	6	A

Onderwijstalen

Nederlands

Trefwoorden

Snelle vermenigvuldiging, modulaire algoritmen, grootste gemene deler, priemtesten, algebra van polynomen, factorisatie van getallen en veeltermen, Gröbnerbasissen

Situering

Dit vak vormt een inleiding tot een gebied dat als "computeralgebra" omschreven kan worden. In deze cursus worden uitsluitend algoritmen bestudeerd voor exacte berekeningen. Deze algoritmen sluiten aan bij de kennis algebra uit de bachelor opleiding.
Het doel is tweevoudig. De studenten moeten deze algoritmen bestuderen en ze moeten vanuit hun theoretische kennis algoritmen leren opstellen voor bepaalde problemen.

Inhoud

De studie van typische algoritmen staat centraal in deze cursus. Na een inleiding tot het vakgebied en de bespreking van enkele technische aspecten zoals datarepresentatie, komen er algoritmen aan bod die we als volgt kunnen indelen.

1 Fundamentele algoritmen: representatie van getallen en polynomen, optelling van getallen en polynomen. Klassieke algoritmen voor vermenigvuldiging, deling en machtsverheffing. Het uitgebreid algoritme van Euclides voor de grootste gemene deler en toepassingen. De Chinese reststelling.

2 Snellere algoritmen voor vermenigvuldiging: algoritme van Karatsuba, Fast Fourier Transformatie, en het algoritme van Schönhage en Strassen. Deling met rest d.m.v. Newton iteratie.

3 Algoritmen voor de grootste gemene deler: grootste gemene deler van polynomen over een UFD. Modulaire algoritmen: een big prime algoritme voor het UFD F[X,Y], F een veld en Z[X], een small prime algoritme voor Z[X].

4 Priemtesten en factorisatie van gehele getallen: de rho-methode van Pollard, de kwadratische zeef; toepassing: RSA.

5 Factorisatie van polynomen: kwadraatvrije factorisatie, factorisatie over eindige velden. Een big prime algoritme voor factorisatie in Z[X], het Hensel lifting

algoritme en het algoritme van Zassenhaus voor factorisatie in Z[X]. Indien de tijd het toelaat: het LLL algoritme met als toepassing een efficiëntere versie van het algoritme van Zassenhaus voor factorisatie in Z[X].

6 Gröbnerbasissen voor polynoomidealen, en toepassingen: o.a. automatische bewijsvoering.

Begincompetenties

Basiskennis algebra (veeltermringen, idealen, eindige velden) en programmeren. Voor bachelors wiskunde: de vakken "Algebra I" en "Practicum Wiskunde" bevatten alle nodige voorkennis. Voor bachelors informatica: de vakken "Lineaire algebra en meetkunde", "Discrete wiskunde" en "Programmeren I" bevatten alle nodige voorkennis.

Eindcompetenties

1 Algoritmen uit de cursus kunnen uitleggen.

2 Wiskundige kennis uit algebra kunnen analyseren en kunnen omzetten naar algoritmen.

3 Resultaten verkregen door middel van computeralgebrasystemen kunnen beoordelen.

Creditcontractvoorwaarde

Toelating tot dit opleidingsonderdeel via creditcontract is mogelijk mits gunstige beoordeling van de competenties

Examencontractvoorwaarde

Dit opleidingsonderdeel kan niet via examencontract gevolgd worden

Didactische werkvormen

Werkcollege, Hoorcollege

Toelichtingen bij de didactische werkvormen

Een volledige syllabus, inclusief een oefeningenpakket worden voorzien.

Studiemateriaal

Type: Syllabus

Naam: Computeralgebra
Richtprijs: Gratis of betaald door opleiding
Optioneel: nee
Taal : Nederlands
Aantal pagina's : 203
Beschikbaar op Ufora : Ja
Online beschikbaar : Ja
Beschikbaar in de bibliotheek : Nee
Beschikbaar via studentenvereniging : Nee

Referenties

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

Vakinhoudelijke studiebegeleiding

Tijdens de hoorcolleges worden de algoritmen volledig uitgelegd. Tijdens de oefeningensessies worden de algoritmen geïllustreerd.

Evaluatiemomenten

periodegebonden en niet-periodegebonden evaluatie

Evaluatievormen bij periodegebonden evaluatie in de eerste examenperiode

Mondelinge evaluatie

Evaluatievormen bij periodegebonden evaluatie in de tweede examenperiode

Mondelinge evaluatie

Evaluatievormen bij niet-periodegebonden evaluatie

Werkstuk

Tweede examenkans in geval van niet-periodegebonden evaluatie

Examen in de tweede examenperiode is mogelijk

Toelichtingen bij de evaluatievormen

Periodegebonden evaluatie: schrijftelijk open boek.

Niet-periodegebonden evaluatie: presentatie en project.

Eindscoreberekening

Periodegebonden evaluatie (50%) + niet-periodegebonden evaluatie (50%).
In geval van niet-slagen kan de student nadien de kans krijgen om een gelijkaardige project uit te voeren voor de niet-periodegebonden evaluatie.