

Rapport for emne MAT4240

Stadiuminfo:	Utkast (S1)
Sist endret:	28.08.2020 Annika Rigenholt (annikap)
Opprettet i EpN:	Ja

Generelt

Emnekodeforslag	MAT4240
Versjonskodeforslag	1
Studienivå	
Administrativt sted	
Studieansvarlig sted	
Vekting	10.0
Vektingstype	Studiepoeng
Navn - bokmål	Elliptiske kurver
Navn - engelsk	Elliptic curves
Første undervisningstermin	2021 VÅR
Siste undervisningstermin	
Første eksamenstermin	

Rapportering

Tilknyttede studieprogram

Undervisning

Undervisningsspråk	Norsk (engelsk på forespørsel)
Undervisningstermin beskrivelse	

Kommentarer

Tidspunkt	Bruker	Tekst
28.08.2020 11:11	Annika Rigenholt (annikap)	Emneinfo: Lagt til fellestekst om Opptak til emnet.; (S1)
28.08.2020 11:08	Annika Rigenholt (annikap)	Emneinfo: Oppdatert med fellestekster om undervisning, eksamen, karakterskala, oblig, adgang til ny-utsatt, undervisningssemester (NRBRT). ; (S1)
25.06.2020 08:32	Kristian Ranestad (ranestad)	Generelt: NRBRT; (S1)

Emneinfo

Kort om emnet

Bokmål:

Emnet gir en innføring i elliptiske kurver, et emne som er sentralt i tallteori, algebraisk geometri, og med anvendelser i datasikkerhet/kryptografi.

Engelsk:

The course gives an introduction to elliptic curves, at central topic in number theory and in algebraic geometry with applications in data security/cryptography.

Hva lærer du?

Bokmål:

Etter å ha fullført emnet:

- kjenner du Weierstrasskurver og elliptiske kurver som tredjegradskurver i planet med koeffisienter i endelige eller uendelige kropp
- kan du regne med gruppestrukturen til elliptiske kurver
- kjenner du sammenhengen mellom komplekse elliptiske kurver og rang to gitter i det komplekse planet
- kjenner du endomorfiringen til elliptiske kurver og isogenier mellom disse
- kjenner du sammenhengen mellom j -invarianten og isomorfiklasser av elliptiske kurver
- kjenner du Hasses teorem for antall punkter på elliptiske kurver over en endelig kropp.

Engelsk:

After completing the course

- you know Weierstrasscurves and elliptic curves as cubic curves in the plane with coefficients in a finite or an infinite field.
- you can perform computations in the group of points on an elliptic curve.
- you know the relation between complex elliptic curves and rank two lattices in the complex plane.
- you know the endomorphism ring of elliptic curves and isogenies between these.
- you know the relation between the j -invariant and isomorphism classes of elliptic curves.
- you know the Hasse theorem for the number of points on elliptic curves over a finite field.

Opptak til emnet

Bokmål:

Studenter tatt opp til andre masterprogrammer kan, etter søknad, få adgang til emnet hvis dette er klarert med eget program.

Dersom du ikke allerede har studieplass ved UiO, kan du søke om opptak til våre studieprogrammer, eller søke om å bli enkeltemnestudent.

Engelsk:

Students admitted at UiO must apply for courses in Studentweb. Students enrolled in other Master's Degree Programmes can, on application, be admitted to the course if this is cleared by their own study programme.

Nordic citizens and applicants residing in the Nordic countries may apply to take this course as a single course student.

If you are not already enrolled as a student at UiO, please see our information about admission requirements and procedures for international applicants.

Anbefalte forkunnskaper

Bokmål:

MAT4200

Engelsk:

MAT4200

Overlappende emner

Bokmål:

5 stp overlapp med MAT4210

Bakgrunnstoff om varieteter og kurver er felles med MAT4210.

Engelsk:

5 stp overlap with MAT4210

Background material on varieties and curves is also part of MAT4210.

Undervisning

Bokmål:

3 timer forelesning/regneøvelse hver uke hele semesteret.

Emnet kan undervises på norsk dersom foreleser og alle studenter på første forelesning ønsker det.

Ved fremmøte av tre eller færre studenter kan faglærer, sammen med undervisningsleder, gjøre emnet om til selvstudiumsemne med veiledning.

Engelsk:

3 hours of lectures/exercises per week throughout the semester.

The course may be taught in Norwegian if the lecturer and all students at the first lecture agree to it.

Upon the attendance of three or fewer students, the lecturer may, in conjunction with the Head of Teaching, change the course to self-study with supervision.

Eksamen

Bokmål:

Avsluttende muntlig eksamen som teller 100 % ved sensurering.

Dette emnet har 1 obligatorisk øvelse som må være godkjent før avsluttende eksamen.

Engelsk:

Final oral exam which counts 100 % towards the final grade.

This course has 1 mandatory assignment that must be approved before you can sit the final exam.

Karakterskala

Bokmål:

Emnet bruker karakterskala fra A til F, der A er beste karakter og F er stryk. Les mer om karakterskalaen.

Engelsk:

Grades are awarded on a scale from A to F, where A is the best grade and F is a fail. Read more about the grading system.

Adgang til ny eller utsatt eksamen

Bokmål:

Dette emnet tilbyr både utsatt og ny eksamen. Les mer:

- Syk på eksamen / utsatt eksamen
- Trekk under eksamen / ta eksamen på nytt

Engelsk:

This course offers both postponed and resit of examination. Read more:

- Illness at exams / postponed exams
- Withdrawal during an examination / Resitting an examination

Undervisningssemester

Bokmål:

Når behov og ressurser tilsier det. Kontakt studieinfo@math.uio.no hvis du er interessert i emnet.

Engelsk:

Taught according to demand and resources. Contact studieinfo@math.uio.no if you are interested in this course.