MA426-15 Elliptic Curves

26/27

Department
Warwick Mathematics Institute
Level
Undergraduate Level 4
Module leader
Harry Schmidt
Credit value
15
Module duration
10 weeks
Assessment
Multiple
Study location
University of Warwick main campus, Coventry

Description

Introductory description

See principle module aims.

Module web page

Module aims

The aims of this module are to introduce the group law on elliptic curves and understand its structure as an abelian group. This is achieved from several points of view. Analytically, via Weierstrass p-functions, algebraically, via endomorphisms and isogenies and arithmetically, via the Mordell-Weil Theorem.

Outline syllabus

This is an indicative module outline only to give an indication of the sort of topics that may be covered. Actual sessions held may differ.

We hope to cover the following topics in varying levels of detail:

1. Non-singular cubics and the group law; Weierstrass equations.
2. Elliptic curves over the rationals; descent, bounding E()/2E(), heights and the Mordell-Weil

theorem, torsion groups; the Nagell-Lutz theorem.
3. Elliptic curves over complex numbers, elliptic functions.
4. Elliptic curves over finite fields; Hasse estimate, application to public key cryptography.
5. Application to diophantin equations: elliptic diophantine problems, Fermat's Last Theorem.
6. Application to integer factorisation: Pollard's p–1 method and the elliptic curve method.

Learning outcomes

By the end of the module, students should be able to:

- The students are expected to become familiar with the group law on elliptic curves, the degree of an isogeny, the parallelogram identity, elliptic curves over finite fields, the Reduction Theorem and the Lutz-Nagell Theorem, explicit 2-descents in the presence of a 2-torsion point and computations of the Mordell-Weil group.

Subject specific skills

Elliptic curves are at the heart of modern number theory, drawing tools from commutative algebra, algebraic geometry, complex analysis, abstract algebra. The students taking this module develop and strengthen the knowledge acquired in their mathematical studies. Moreover, elliptic curves find applications in cryptography and are used in encoding and decoding of messages sent over the internet.

Transferable skills

Elliptic curves are at the heart of modern number theory, drawing tools from commutative algebra, algebraic geometry, complex analysis, abstract algebra. The students taking this module develop and strengthen the knowledge acquired in their mathematical studies. Moreover, elliptic curves find applications in cryptography and are used in encoding and decoding of messages sent over the internet.

Study

Study time

Type	Required
Lectures	30 sessions of 1 hour (20%)
Tutorials	9 sessions of 1 hour (6%)
Private study	111 hours (74%)
Total	150 hours

Private study description

Review lectured material and work on set exercises.

Costs

No further costs have been identified for this module.

Assessment

You do not need to pass all assessment components to pass the module.

Students can register for this module without taking any assessment.

Assessment group D1

	Weighting	Study time	Eligible for self-certification
Assessment Coursework	15%		No
Centrally-timetabled examination (On-campus) 3 hour exam, no books allowed	85%		No

---

- Answerbook Gold (24 page)

Assessment group R

	Weighting	Study time	Eligible for self-certification
In-person Examination - Resit	100%		No

- Answerbook Gold (24 page)

Feedback on assessment

Marked coursework and exam feedback.

Past exam papers for MA426

Availability

Courses

This module is Optional for:

- TMAA-G1PE Master of Advanced Study in Mathematical Sciences
  - Year 1 of G1PE Master of Advanced Study in Mathematical Sciences
  - Year 1 of G1PE Master of Advanced Study in Mathematical Sciences
- Year 1 of TMAA-G1PD Postgraduate Taught Interdisciplinary Mathematics (Diploma plus MSc)
- Year 1 of TMAA-G1P0 Postgraduate Taught Mathematics
- TMAA-G1PC Postgraduate Taught Mathematics (Diploma plus MSc)
  - Year 1 of G1PC Mathematics (Diploma plus MSc)
  - Year 2 of G1PC Mathematics (Diploma plus MSc)

This module is Core option list F for:

- Year 4 of UMAA-GV19 Undergraduate Mathematics and Philosophy with Specialism in Logic and Foundations

This module is Option list A for:

- TMAA-G1PD Postgraduate Taught Interdisciplinary Mathematics (Diploma plus MSc)
  - Year 1 of G1PD Interdisciplinary Mathematics (Diploma plus MSc)
  - Year 2 of G1PD Interdisciplinary Mathematics (Diploma plus MSc)
- Year 1 of TMAA-G1P0 Postgraduate Taught Mathematics
- Year 1 of TMAA-G1PC Postgraduate Taught Mathematics (Diploma plus MSc)
- Year 4 of USTA-G1G3 Undergraduate Mathematics and Statistics (BSc MMathStat)

This module is Option list B for:

- TMAA-G1PD Postgraduate Taught Interdisciplinary Mathematics (Diploma plus MSc)
  - Year 1 of G1PD Interdisciplinary Mathematics (Diploma plus MSc)
  - Year 2 of G1PD Interdisciplinary Mathematics (Diploma plus MSc)
- Year 1 of TMAA-G1PC Postgraduate Taught Mathematics (Diploma plus MSc)
- Year 4 of UCSA-G4G3 Undergraduate Discrete Mathematics
- Year 5 of UCSA-G4G4 Undergraduate Discrete Mathematics (with Intercalated Year)

This module is Option list C for:

- UMAA-G105 Undergraduate Master of Mathematics (with Intercalated Year)
  - Year 3 of G105 Mathematics (MMath) with Intercalated Year
  - Year 4 of G105 Mathematics (MMath) with Intercalated Year
  - Year 5 of G105 Mathematics (MMath) with Intercalated Year
- UMAA-G103 Undergraduate Mathematics (MMath)
  - Year 3 of G103 Mathematics (MMath)
  - Year 4 of G103 Mathematics (MMath)
- Year 4 of UMAA-G107 Undergraduate Mathematics (MMath) with Study Abroad
- UMAA-G106 Undergraduate Mathematics (MMath) with Study in Europe

    - Year 3 of G106 Mathematics (MMath) with Study in Europe
    - Year 4 of G106 Mathematics (MMath) with Study in Europe

This module is Option list E for:

- Year 5 of USTA-G301 Undergraduate Master of Mathematics,Operational Research,Statistics and Economics (with Intercalated