23MAC260 Elliptic Curves: Definitions and Theorems List

Last updated March 20, 2024

The following list includes all definitions and theorem statements that you may be asked to reproduce in the exam. The references in brackets tell you where to find these in the module materials.

Remember that **all** module material is examinable unless clearly marked otherwise!

Definitions

- Elliptic curve (W1)
- Order of a point on an elliptic curve (see "Abelian groups reminder" document)
- Isomorphism of elliptic curves (W4)
- Torsion subgroup of an elliptic curve defined over $\mathbb{Q}$ (W5)
- Height function h_x (W7)
- Weierstrass $\wp$-function associated to a lattice (W8)
- Eisenstein series of weight k associated to a lattice (W9)

Theorems

- Mordell's Theorem (W5)
- Integrality Theorem (W5)
- Nagell–Lutz Theorem (W5)
- Torsion Embedding Theorem + Week 6 Corollary 1.6 (W6)
- Equivalence Theorem, Parts 1 and 2 (W9)
- Similarity Theorem, Parts 1 and 2 (W10)
- Fundamental Domain Theorem (W10)