Information about the elliptic curve exam

You will sit a 3 hour exam which counts for 100% of the module mark.

In general

The points attributed to one question do not necessarily indicate how difficult the question is. I tried to balance the points in such a way that I hope no scaling will be needed in the end.

There are three types of questions:

- Bookwork question will ask to write down a definition or a statement form the lecture notes. (You can ignore definitions given in problem sheets like the j-invariant).
- Questions using methods from the notes and similar to questions in the problem classes.
- Unseen questions, a bit like the harder questions on the problem sheets.

In particular there is no need to learn any of the proof from the notes by heart. You are allowed to use a calculator. For any question, you may use any proven result from the notes (unless otherwise stated).

Examinable/non-examinable material

Here is a list with comments on what is examinable and what not. The list is not completely exhaustive in all details, but should give a rough guide of what methods and concepts should be studied carefully.

- I will not ask anything about chapter 1. The methods from the introduction of course come up later again anyway.
- There will be no question about chapter 2.
- All material from chapter 3 is examinable. You should be able to work with projective coordinates and projective lines both as linear equation as well as parametrisations. The lecture notes describe how to intersect lines and how to find lines through given points; but the examples on the problem sheets and in the coursework give different methods which are useful to know about.
- All of chapter 4 is examinable. You should know how to go from affine curves to projective curves and back.

- It is good to know what conics and degenerate conics are, how to intersect conics with lines and how to find the parametrisation of a non-degenerate conic C with a point $P \in C(k)$. Note for this last point, one needs to know the first part of the proof of Theorem 4.4; the tangent however is better explained later.

- One needs to know the definition of intersection multiplicities $I_P(C, L)$ for curves C and lines L. You should be able to compute this for any C and L and P.

- For inflection points and singular points it is important to know the definition and that one can check singular points using partial derivatives as in Theorem 4.6. In a given example one should be able to determine if a projective curve is smooth.

- Bézout's theorem and Theorem 4.8 are important to know. The proof of the latter is not important while the proof of Bézout's theorem is about intersecting a line with a curve, which one should be able to do in an example. You do not need to know the general version of Bézout's theorem.

- The non-examinable part of chapter 5 is the proof of the associativity including Chasles' theorem and section 5.4.

- A part from the general definition of an elliptic curve one should know how to check quickly if a Weierstrass equation is an elliptic curve using the discriminant. Of course the group law (addition, duplication and inverses) with its special cases should be fully understood for a general smooth cubic. It is good to know why O is the identity element, why the group law is closed, abelian and why the construction of the inverse gives the inverse indeed. One should be able to use that the group law is associative, but there is no need to know why it is so.

- It is very good to remember how to add, find the inverse and duplicate points on an elliptic curve in Weierstrass form $y^2 = x^3 + A\,x + B$. You should also understand how this procedure (or formulae) are obtained so that you find this for a different, more general form of an elliptic curve like $y^2 = x^2 + a\,x^2 + b\,x$ or so.

- For small p, you should be able to determine the group structure and generators for an elliptic curve in Weierstrass form over $\mathbb{F}_p$.

- One should remember the precise definition of the reduction map and that it is a group homomorphism. It is good to know that a point on $E(\mathbb{Q})$ in Weierstrass form can be written as $\left(\frac{a}{e^2}, \frac{b}{e^3}\right)$ with integers a, b, e and why this is the case.

- In chapter 6, it is section 6.4 which is not examinable.
- Knowing what torsion points are, how to recognise 2-torsion and 3-torsion points on a Weierstrass equation are important.
- From section 6.2, one should know that torsion points have integral coordinates and that reduction map is injective on torsion points for primes of good reduction. Also how one can use this to bound the number of torsion points in $E(\mathbb{Q})$.
- You should know the theorem of Lutz-Nagell and how to use it to determine all torsion points in $E(\mathbb{Q})$ on a Weierstrass equation.
- However, there is no need to learn anything about the proof of Lemma 6.3 or the proof of Corollary 6.4
- The Kummer maps κ_i should be remembered and how to evaluate them on points in $E(\mathbb{Q})$. One should know the basic properties of κ_i as in Propositions 7.1, 7.2 and 7.4, but you do not need to know about the proofs of these. In particular you are not asked to know Lemma 7.3 and how to find Q such that $2Q = P$.
- Of section 7.2 you should remember the definition of the height and that there are finitely many points of bounded height (Lemma 7.6), but you may ignore the properties like Lemma 7.7 and 7.8.
- It is important to know the statement of Mordell's theorem and what it implies, however no knowledge about the proof is needed for the exam.
- None of chapter 8 is examinable.

On exams of previous years

The content of the module has changed quite a bit with respect to how it was taught two years ago, but it is similar to last year. Some of the notations and assumptions have changed. I put on moodle a commented and reformatted version of the exam in 2016/17. Please consult this together with the original questions and solution. Also in 2017/18, section 7.3 was not examinable, but it was last year and it is this year.