Julian Lyczak's web page

Elliptic curves, autumn 2015

This is the web page of the DIAMANT / Mastermath course Elliptic Curves.

Notification

Your exams and retakes have been marked. Contact Djordjo for your grade. You can find the email address below.
If you want to see your exam make an appointment with one of the lecturers.

Organization

Lecturers:	Marco Streng	streng (at) math.leidenuniv.nl	Snelliusgebouw room 229
	Martin Bright	m.j.bright (at) math.leidenuniv.nl	Snelliusgebouw room 252
Problem session:	Peter Koymans	p.h.koymans (at) math.leidenuniv.nl	Snelliusgebouw room 227
	Julian Lyczak	j.t.lyczak (at) math.leidenuniv.nl	Snelliusgebouw room 242
	Djordjo Milovic	dzm656 (at) gmail.com	Snelliusgebouw room 227
	Carlo Pagano	carlein90 (at) gmail.com	Snelliusgebouw room 242
	Pavel Solomatin	pavelsolomatin179 (at) gmail.com	Snelliusgebouw room 238

Do NOT send in your homework to these email addresses.
Homework is to be handed in using: mastermathec (at) gmail.com. See below for more information on handing in homework.

Location:	VU Amsterdam
Room:	WN-C121 Apart from the lecture on December 8: WN-P323
Time:	Tuesdays, 10:15--13:00
	"WN" means "Wis- en Natuurkundegebouw", Vrije Universiteit, De Boelelaan 1081a, Amsterdam. The arrow on this map points to an entrance.
	The "Snelliugebouw" is the building of the mathematics departement in Leiden, Niels Bohrweg 1 2333CA, Leiden. map

On the 8th and 9th of September we will start with an Intensive Course Categories and Modules. This will also be at the Vrije Universiteit in Amsterdam but in different rooms.

September 8	
11:00-13:00	WN-M655
14:00-16:00	WN-C147
September 9	
11:00-13:00	WN-F647
14:00-16:00	WN-M655

Aim

Along various historical paths, the origins of elliptic curves can be traced to calculus, complex analysis and algebraic geometry, and their arithmetic aspects have made them key objects in modern cryptography and in Wiles's proof of Fermat's last theorem. This course is an introduction to both the theoretical and the computational aspects of elliptic curves.

Description

The topics treated include a general discussion of elliptic curves and their group law, Diophantine equations in two variables, and Mordell's theorem. We will also discuss elliptic curves over finite fields with applications such as factoring integers, elliptic discrete logarithms, and cryptography. We will pursue both a theoretical and a computational approach.

Examination

The final grade will be 20% of the average homework grade plus 80% of the grade for the final exam.

The final exam is a traditional closed-book written exam, and will take place on

~~Tuesday the 5th of January, 12:00-15:00 at the VU, TenT Blok 1.~~

Tuesday the 5th of January, 10:00-13:00 at the VU, MF FG1.

The retake will be on

Tuesday the 26th of January, 12:00-15:00 at the VU, WN-Q112.

Homework must be handed in before the beginning of the lecture. Homework that is not handed in in time will get the grade 1 (out of 10). The lowest 2 homework grades do not count.

You can either hand in a paper version of your homework before the start of the lecture or via the email address mastermathec (at) gmail.com. If you choose to do the latter, you have to TeX your work and send us the corresponding PDF file. Students handing in there work on paper are also strongly encouraged to use TeX or LaTeX. In all cases make sure that your name, university and student number are clearly presented at the top of the first page.
Note that this email address is only for handing in homework! For any other questions related to the course, contact one of the lecturers or teaching assistents.

If you wish to work together (which we encourage), then you must write up your answers individually. Almost identical answers will not be accepted.

Schedule

#	Date	Subject	Homework
1	15 September	*1. Introduction* MB: introduction to elliptic curves *2. Basic algebraic geometry* MS: affine algebraic sets, correspondense with ideals, Nullstellensatz, irreducibility, coordinate rings, function fields. [Fulton] Sections 1.2, 1.3, (1.4,) 1.5, (1.6,) 1.7, 2.1, 2.4	Exercises
2	22 September	MS: projective space, plane projective curves, tangent lines and smoothness, intersection numbers and Bézout's theorem, Weierstrass equations, elliptic curves, group law, coordinate change of Weierstrass equations, discriminant of a Weierstrass equation, short Weierstrass equation [Milne] Sections 1.1 and 1.3 (alternatively, see [Fulton] Chapters 3 and 4, [Silverman] III.1 and III.2) Perspective drawing projective plane and Projective plane curve	Exercises
3	29 September	*3. Elliptic curves over the complex numbers* MB: Complex tori and elliptic functions [Milne] Chapter 3.1 and 3.2, and [Stevenhagen] Chapter 2	Exercises
4	6 October	MB: Elliptic curves over the complex numbers [Milne] Chapter 3.3 and [Stevenhagen] Chapter 3	Exercises
5	13 October	*4. The Riemann-Roch theorem* MS: function field, order of a function at a point, local ring at a smooth point is discrete valuation ring, divisor, Picard group, the Riemann-Roch theorem, genus [Milne] Section I.4 and [Fulton] Theorem 1 in Section 3.2. Alternatively, the corresponding parts of [Fulton], [Silverman] or [Stichtenoth].	Exercises
6	20 October	*5. Homomorphisms* MB: Morphisms of curves, differentials and the canonical divisor, the general definition of an elliptic curve, description of the group law in terms of the Picard group [Milne] (rest of sections I.4 and II.1), [Fulton] (6.3, 6.6, 8.4, 8.5), [Silverman] (I.3, II.2, II.4, III.3).	Exercises
7	27 October	MS: curve morphisms, ramification index, separability, (in)separable degree, isogenies, endomorphism ring [Silverman] Section II.2 (esp. II.2.6, II.2.12), Proposition II.3.6, Proposition II.4.2, Section III.4 up to Corollary 4.9. Note: I will probably not write tex-ed notes, so those who do not have the book are advised to take notes.	Exercises
8	3 November	MS: isogenies, dual isogeny, degrees of isogenies, structure of the n-torsion subgroup E[n], Hasse's theorem (in the homework) [Silverman] Sections III.4, 5, 6 and maybe some more. Note: I will probably not write tex-ed notes, so those who do not have the book are advised to take notes.	Hand in 45b, 49, 50 from the previous homework sheet.
9	10 November	*6. The Mordell-Weil theorem* MB: Mordell-Weil theorem, 2-descent, heights, proof of Mordell's theorem (part 1)	Exercises
10	17 November	MB: Mordell-Weil theorem, 2-descent, heights, proof of Mordell's theorem (part	Exercises Update in homework problem 61:

		2)	find the rank and the 2-torsion.
11	24 November	*7. Algorithmic applications* MS: Elliptic curve cryptography (slides), the elliptic curve factoring method (IV.4 in [Silverman-Tate] or Wikipedia), and elliptic curve primality proving (Top's notes or Wikipedia). Alternatively, all these topics (and much more) are treated in detail in [HEHCC] and (except for primality proving) [HPS].	Exercises
12	1 December	*8. Reduction and torsion* MB: Reduction of elliptic curves and torsion subgroups of the rational points	Exercises
13	8 December	*9. Computer class* MS: Computer class in SageMath **The lecture is in room WN-P323.** In case we do not get access to the VU computers, we would like to ask you to bring a laptop if possible, and to install eduroam OR Sagemath on that laptop. In order to save time, please create an account on sage.math.leidenuniv.nl beforehand. To prepare for the computer class, you can have a look at instructions from two years ago or Sage's homepage. A worksheet to learn Sage. You can also find the same file "basic Sage" online.	Download the final homework here. You can also find the same file "Elliptic curves, mastermath 2015" online. Deadline 15 December Correction on problem 10: Let $\overline{E_2}$ denote the reduction of E_2 modulo 5. The result of Exercise 6 shows that $\overline{E_2}$ is an elliptic curve over the field $\mathbf{F}_5$ of 5 elements. Exercise 10: Use the number of points of $\overline{E_2}$ over $\mathbf{F}_5$ to show that in $\mathrm{End}(\overline{E_2})$, we have $\mathrm{Frob} = [-1] + [2i]$ for some square root $[2i]$ of $[-4]$. Answer: (just text, no Sage)
14	15 December	*10. The conjecture of Birch and Swinnerton-Dyer* final lecture	We will discuss the practice exam during exercise class.

Prerequisites

Group, ring and field theory (cf. the Leiden syllabi Algebra 1, 2 and 3 found here) and complex variables.

Literature

[Cassels] **J.W.S. Cassels:** ***Lectures on Elliptic Curves*** §§2–5 for the local-global principle, and §14 for 2-descent. Here is a scanned copy of §§2–6, 10 and 18, here of §§6–9, here of §§10–12, and here is one of §14.

[Cohen-Stevenhagen] **H. Cohen** and **P. Stevenhagen** - *Computational class field theory*. Chapter 15 in the following book on *algorithmic number theory*. See pages 518--519 for how to enumerate all lattices having CM by a given ring.

[Fulton] **W. Fulton:** ***Algebraic Curves - An Introduction to Algebraic Geometry*** is out of print but available online.

[HEHCC] ***Handbook of elliptic and hyperelliptic curve cryptography*** edited by **Cohen, Henri and Frey, Gerhard and Avanzi, Roberto and Doche, Christophe and Lange, Tanja and Nguyen, Kim and Vercauteren, Frederik.** Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL. 2006, ISBN: 978-1-58488-518-4 or ISBN: 1-58488-518-1.

[HPS] **Jeffrey Hoffstein and Jill Pipher and Joseph H. Silverman:** ***An introduction to mathematical cryptography.*** Undergraduate Texts in Mathematics, Springer, New York. 2008. ISBN: 978-0-387-77993-5.
For those whose university has a Springerlink subscription (e.g. Leiden), the book is downloadable for free from within the university network from here.

[Milne] **J.S. Milne:** ***Elliptic Curves*** is electronically available online and (according to the book's web page) the paperback version costs only $17. Section IV.9 is a good reference for the Zeta function of a curve.

[Silverman-Tate] Newcomers to the subject are suggested to buy the book **J.H. Silverman and J. Tate:** ***Rational Points on Elliptic Curves.*** Undergraduate Texts in Mathematics, Springer-Verlag, Corr. 2nd printing, 1994, ISBN: 978-0-387-97825-3: it contains a lot of the material treated in the course.

[Silverman1] Advanced students with a good knowledge of algebraic geometry are recommended to (also) buy **J.H. Silverman:** ***The arithmetic of elliptic curves.*** Corrected reprint of the 1986 original. Graduate Texts in Mathematics, 106. Springer-Verlag, New York, 1992. ISBN: 0-387-96203-4.

[Silverman2] Further references: **J.H. Silverman:** ***Advanced topics in the arithmetic of elliptic curves.*** Graduate Texts in Mathematics 151, Springer-Verlag, 1994. ISBN: 0-387-94328-5.

[de Smit-Stevenhagen] Notes (in English) by Bart de Smit en Peter Stevenhagen on elliptic curves: **P. Stevenhagen & B. de Smit:** ***Kernvak algebra.*** PDF

[Stevenhagen] Lecture notes by Peter Stevenhagen: **P. Stevenhagen:** ***Complex Elliptic Curves.*** PDF

[Stichtenoth] Book by Stichtenoth on function fields and coding theory.
For those whose university has a Springerlink subscription (e.g. Leiden), the book is downloadable for free from within

the university network from here.

Last change: 11/21/2018 13:07:08.