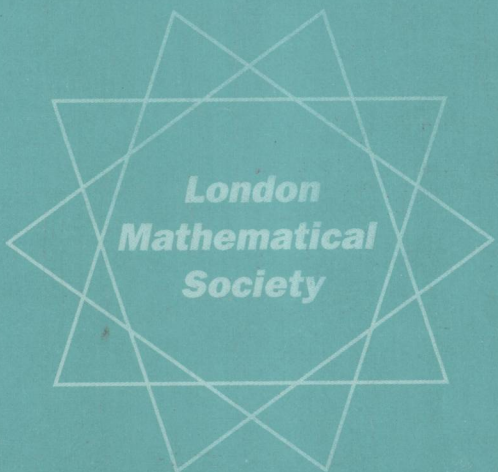
London Mathematical Society
Lecture Note Series 341

Ranks of Elliptic Curves and Random Matrix Theory

Edited by J. B. Conrey, D. W. Farmer, F. Mezzadri, and N. C. Snaith



AMBRIDGE
VERSITY PRESS

London Mathematical Society Lecture Note Series: 341

Ranks of Elliptic Curves and Random Matrix Theory

Edited by

J. B. Conrey
American Institute of Mathematics

D. W. Farmer
American Institute of Mathematics

F. Mezzadri
University of Bristol

N. C. Snaith
University of Bristol

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town, Singapore, São Paulo

Cambridge University Press
The Edinburgh Building, Cambridge CB2 2RU, UK

Published in the United States of America by Cambridge University Press, New York

www.cambridge.org
Information on this title: www.cambridge.org/9780521699648

First published 2007

Printed in the United Kingdom at the University Press, Cambridge

A catalogue record for this publication is available from the British Library

ISBN-13 978-0-521-69964-8 paperback

LONDON MATHEMATICAL SOCIETY LECTURE NOTE SERIES

Managing Editor: Professor N.J. Hitchin, Mathematical Institute, University of Oxford, 24-29 St Giles, Oxford OX1 3LB, United Kingdom

The titles below are available from booksellers, or from Cambridge University Press at www.cambridge.org/mathematics

214 Generalised Euler-Jacobi inversion formula and asymptotics beyond all orders, V. KOWALENKO *et al*
215 Number theory 1992–93, S. DAVID (ed)
216 Stochastic partial differential equations, A. ETHERIDGE (ed)
217 Quadratic forms with applications to algebraic geometry and topology, A. PFISTER
218 Surveys in combinatorics, 1995, P. ROWLINSON (ed)
220 Algebraic set theory, A. JOYAL & I. MOERDIJK
221 Harmonic approximation., S.J. GARDINER
222 Advances in linear logic, J.-Y. GIRARD, Y. LAFONT & L. REGNIER (eds)
223 Analytic semigroups and semilinear initial boundary value problems, KAZUAKI TAIRA
224 Computability, enumerability, unsolvability, S.B. COOPER, T.A. SLAMAN & S.S. WAINER (eds)
225 A mathematical introduction to string theory, S. ALBEVERIO, *et al*
226 Novikov conjectures, index theorems and rigidity I, S. FERRY, A. RANICKI & J. ROSENBERG (eds)
227 Novikov conjectures, index theorems and rigidity II, S. FERRY, A. RANICKI & J. ROSENBERG (eds)
228 Ergodic theory of $\mathbf{Z}^d$ actions, M. POLLICOTT & K. SCHMIDT (eds)
229 Ergodicity for infinite dimensional systems, G. DA PRATO & J. ZABCZYK
230 Prolegomena to a middlebrow arithmetic of curves of genus 2, J.W.S. CASSELS & E.V. FLYNN
231 Semigroup theory and its applications, K.H. HOFMANN & M.W. MISLOVE (eds)
232 The descriptive set theory of Polish group actions, H. BECKER & A.S. KECHRIS
233 Finite fields and applications, S. COHEN & H. NIEDERREITER (eds)
234 Introduction to subfactors, V. JONES & V.S. SUNDER
235 Number theory 1993–94, S. DAVID (ed)
236 The James forest, H. FETTER & B. G. DE BUEN
237 Sieve methods, exponential sums, and their applications in number theory, G.R.H. GREAVES *et al*
238 Representation theory and algebraic geometry, A. MARTSINKOVSKY & G. TODOROV (eds)
240 Stable groups, F.O. WAGNER
241 Surveys in combinatorics, 1997, R.A. BAILEY (ed)
242 Geometric Galois actions I, L. SCHNEPS & P. LOCHAK (eds)
243 Geometric Galois actions II, L. SCHNEPS & P. LOCHAK (eds)
244 Model theory of groups and automorphism groups, D. EVANS (ed)
245 Geometry, combinatorial designs and related structures, J.W.P. HIRSCHFELD *et al*
246 p-Automorphisms of finite p-groups, E.I. KHUKHRO
247 Analytic number theory, Y. MOTOHASHI (ed)
248 Tame topology and o-minimal structures, L. VAN DEN DRIES
249 The atlas of finite groups: ten years on, R. CURTIS & R. WILSON (eds)
250 Characters and blocks of finite groups, G. NAVARRO
251 Gröbner bases and applications, B. BUCHBERGER & F. WINKLER (eds)
252 Geometry and cohomology in group theory, P. KROPHOLLER, G. NIBLO & R. STÖHR (eds)
253 The q-Schur algebra, S. DONKIN
254 Galois representations in arithmetic algebraic geometry, A.J. SCHOLL & R.L. TAYLOR (eds)
255 Symmetries and integrability of difference equations, P.A. CLARKSON & F.W. NIJHOFF (eds)
256 Aspects of Galois theory, H. VÖLKLEIN *et al*
257 An introduction to noncommutative differential geometry and its physical applications 2ed, J. MADORE
258 Sets and proofs, S.B. COOPER & J. TRUSS (eds)
259 Models and computability, S.B. COOPER & J. TRUSS (eds)
260 Groups St Andrews 1997 in Bath, I, C.M. CAMPBELL *et al*
261 Groups St Andrews 1997 in Bath, II, C.M. CAMPBELL *et al*
262 Analysis and logic, C.W. HENSON, J. IOVINO, A.S. KECHRIS & E. ODELL
263 Singularity theory, B. BRUCE & D. MOND (eds)
264 New trends in algebraic geometry, K. HULEK, F. CATANESE, C. PETERS & M. REID (eds)
265 Elliptic curves in cryptography, I. BLAKE, G. SEROUSSI & N. SMART
267 Surveys in combinatorics, 1999, J.D. LAMB & D.A. PREECE (eds)
268 Spectral asymptotics in the semi-classical limit, M. DIMASSI & J. SJÖSTRAND
269 Ergodic theory and topological dynamics, M.B. BEKKA & M. MAYER
270 Analysis on Lie groups, N.T. VAROPOULOS & S. MUSTAPHA
271 Singular perturbations of differential operators, S. ALBEVERIO & P. KURASOV
272 Character theory for the odd order theorem, T. PETERFALVI
273 Spectral theory and geometry, E.B. DAVIES & Y. SAFAROV (eds)

274 The Mandlebrot set, theme and variations, TAN LEI (ed)
275 Descriptive set theory and dynamical systems, M. FOREMAN *et al*
276 Singularities of plane curves, E. CASAS-ALVERO
277 Computational and geometric aspects of modern algebra, M.D. ATKINSON *et al*
278 Global attractors in abstract parabolic problems, J.W. CHOLEWA & T. DLOTKO
279 Topics in symbolic dynamics and applications, F. BLANCHARD, A. MAASS & A. NOGUEIRA (eds)
280 Characters and automorphism groups of compact Riemann surfaces, T. BREUER
281 Explicit birational geometry of 3-folds, A. CORTI & M. REID (eds)
282 Auslander-Buchweitz approximations of equivariant modules, M. HASHIMOTO
283 Nonlinear elasticity, Y. FU & R.W. OGDEN (eds)
284 Foundations of computational mathematics, R. DEVORE, A. ISERLES & E. SÜLI (eds)
285 Rational points on curves over finite, fields, H. NIEDERREITER & C. XING
286 Clifford algebras and spinors 2ed, P. LOUNESTO
287 Topics on Riemann surfaces and Fuchsian groups, E. BUJALANCE *et al*
288 Surveys in combinatorics, 2001, J. HIRSCHFELD (ed)
289 Aspects of Sobolev-type inequalities, L. SALOFF-COSTE
290 Quantum groups and Lie theory, A. PRESSLEY (ed)
291 Tits buildings and the model theory of groups, K. TENT (ed)
292 A quantum groups primer, S. MAJID
293 Second order partial differential equations in Hilbert spaces, G. DA PRATO & J. ZABCZYK
294 Introduction to the theory of operator spaces, G. PISIER
295 Geometry and Integrability, L. MASON & YAVUZ NUTKU (eds)
296 Lectures on invariant theory, I. DOLGACHEV
297 The homotopy category of simply connected 4-manifolds, H.-J. BAUES
298 Higher operads, higher categories, T. LEINSTER
299 Kleinian Groups and Hyperbolic 3-Manifolds Y. KOMORI, V. MARKOVIC & C. SERIES (eds)
300 Introduction to Möbius Differential Geometry, U. HERTRICH-JEROMIN
301 Stable Modules and the D(2)-Problem, F.E.A. JOHNSON
302 Discrete and Continuous Nonlinear Schrödinger Systems, M. J. ABLORWITZ, B. PRINARI & A. D. TRUBATCH
303 Number Theory and Algebraic Geometry, M. REID & A. SKOROBOGATOV (eds)
304 Groups St Andrews 2001 in Oxford Vol. 1, C.M. CAMPBELL, E.F. ROBERTSON & G.C. SMITH (eds)
305 Groups St Andrews 2001 in Oxford Vol. 2, C.M. CAMPBELL, E.F. ROBERTSON & G.C. SMITH (eds)
306 Peyresq lectures on geometric mechanics and symmetry, J. MONTALDI & T. RATIU (eds)
307 Surveys in Combinatorics 2003, C. D. WENSLEY (ed.)
308 Topology, geometry and quantum field theory, U. L. TILLMANN (ed)
309 Corings and Comodules, T. BRZEZINSKI & R. WISBAUER
310 Topics in Dynamics and Ergodic Theory, S. BEZUGLYI & S. KOLYADA (eds)
311 Groups: topological, combinatorial and arithmetic aspects, T. W. MÜLLER (ed)
312 Foundations of Computational Mathematics, Minneapolis 2002, FELIPE CUCKER *et al* (eds)
313 Transcendental aspects of algebraic cycles, S. MÜLLER-STACH & C. PETERS (eds)
314 Spectral generalizations of line graphs, D. CVETKOVIC, P. ROWLINSON & S. SIMIC
315 Structured ring spectra, A. BAKER & B. RICHTER (eds)
316 Linear Logic in Computer Science, T. EHRHARD *et al* (eds)
317 Advances in elliptic curve cryptography, I. F. BLAKE, G. SEROUSSI & N. SMART
318 Perturbation of the boundary in boundary-value problems of Partial Differential Equations, D. HENRY
319 Double Affine Hecke Algebras, I. CHEREDNIK
321 Surveys in Modern Mathematics, V. PRASOLOV & Y. ILYASHENKO (eds)
322 Recent perspectives in random matrix theory and number theory, F. MEZZADRI & N. C. SNAITH (eds)
323 Poisson geometry, deformation quantisation and group representations, S. GUTT *et al* (eds)
324 Singularities and Computer Algebra, C. LOSSEN & G. PFISTER (eds)
325 Lectures on the Ricci Flow, P. TOPPING
326 Modular Representations of Finite Groups of Lie Type, J. E. HUMPHREYS
328 Fundamentals of Hyperbolic Manifolds, R. D. CANARY, A. MARDEN & D. B. A. EPSTEIN (eds)
329 Spaces of Kleinian Groups, Y. MINSKY, M. SAKUMA & C. SERIES (eds)
330 Noncommutative Localization in Algebra and Topology, A. RANICKI (ed)
331 Foundations of Computational Mathematics, Santander 2005, L. PARDO, A. PINKUS, E. SULI & M. TODD (eds)
332 Handbook of Tilting Theory, L. ANGELERI HÜGEL, D. HAPPEL & H. KRAUSE (eds)
333 Synthetic Differential Geometry 2ed, A. KOCK
334 The Navier-Stokes Equations, P. G. DRAZIN & N. RILEY
335 Lectures on the Combinatorics of Free Probability, A. NICU & R. SPEICHER
336 Integral Closure of Ideals, Rings, and Modules, I. SWANSON & C. HUNEKE
337 Methods in Banach Space Theory, J. M. F. CASTILLO & W. B. JOHNSON (eds)
338 Surveys in Geometry and Number Theory N. YOUNG (ed)

Contents

Number fields and higher twists

Shimura correspondence, and twists

Global structure: Sha and descent

Introduction

J. B. Conrey, D. W. Farmer, F. Mezzadri and N. C. Snaith

The group of rational points on an elliptic curve is a fascinating number theoretic object. The description of this group, as enunciated by Birch and Swinnerton-Dyer in terms of the special value of the associated L-function, or a derivative of some order, at the center of the critical strip, is surely one of the most beautiful relationships in all of mathematics; and it's understanding also carries a $1 million dollar reward!

Random Matrix Theory (RMT) has recently been revealed to be an exceptionally powerful tool for expressing the finer structure of the value-distribution of L-functions. Initially developed in great detail by physicists interested in the statistical properties of energy levels of atomic nuclei, RMT has proven to be capable of describing many complex phenomena, including average behavior of L-functions.

The purpose of this volume is to expose how RMT can be used to describe the statistics of some exotic phenomena such as the frequency of rank two elliptic curves. Many, but not all, of the papers here have origins in a workshop that took place at the Isaac Newton Institute in February of 2004 entitled "Clay Mathematics Institute Special week on Ranks of Elliptic Curves and Random Matrix Theory." The workshop began with the Spittalsfield day of expository lectures, highlighted by reminiscences by Bryan Birch and Sir Peter Swinnerton-Dyer on the development of their conjecture. The week continued with a somewhat free-form workshop featuring discussion sessions, groups working on various problems, and spontaneous lectures. The idea for this volume arose at this workshop. The intention is to gather together a number of articles to assist someone wishing to begin work in this area.

One of the hightlights of this volume is the collection of beautiful expository papers and surveys: Kowalski's introduction to elliptic curves, Silverberg on ranks of elliptic curves, Ulmer's discussion of zeta-functions over function fields, Gamburd's explanation of symmetric function theory, Rodriguez-Villegas on the theta series associated with special values, Delaunay on probabilistic group theory, Farmer on families, and Young on exotic families of elliptic curves. There are an amazingly rich variety of topics arising from this one focus.

The most important invariant of an elliptic curve is the rank of its (Mordell-Weil) group of rational points; it is a non-negative integer, believed to be 0 or 1 for almost all elliptic curves. The catalyst for the Newton Institute workshop was a conjecture (see [CKRS]) about how often the rank is 2 for the family of quadratic twists of a given elliptic curve. Each elliptic curve has an L-function associated with it; this is an entire function which satisfies a functional equation. The Birch and Swinnerton-Dyer conjecture asserts,

among other things, that the order of vanishing at the central point of the L-function associated with an elliptic curve is equal to the rank. It is generally conjectured that almost all elliptic curves have rank zero or one according to whether the sign of the functional equation of the related L-function is $+1$ or -1. Rank two curves should occur with L-functions that have a $+1$ sign of their functional equation but vanish nevertheless at the central point. These are expected to be rare; the question of how rare is the subject here.

If the elliptic curve is given by $E : y^2 = x^3 + Ax + B$, and if d is a fundamental discriminant, then the quadratic twist of E by d is the elliptic curve $E_d := dy^2 = x^3 + Ax + B$. The conjecture, derived from RMT and number theory, is that E_d will have rank 2 for asymptotically $c_E x^{3/4} (\log x)^{b_E}$ values of d with $|d| \le x$. Here b_E is one of four values described in the article by Delaunay and Watkins, whereas c_E is yet to be determined but depends on a mix of RMT, number theory, and probabilistic group theory (see the article of Delaunay on class groups and Tate-Shafarevich groups).

This conjecture, while interesting, is not as compelling as it might be because of our ignorance of c_E. However, an absolutely convincing case for RMT can be given by considering rank 2 curves as above but divided into *arithmetic progressions* of d modulo some prime p.

Using RMT arguments combined with a number theoretic discretization of the problem, one is led to predict that if a is a quadratic residue mod p and b is a quadratic non-residue then the ratio of rank 2 twists among $d \equiv a \bmod p$ to $d \equiv b \bmod p$ is, in the limit,

$$\sqrt{\frac{p+1-a_p}{p+1+a_p}},$$

where $L(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ is the L-function associated with E. Those familiar with the conjecture of Birch and Swinnerton-Dyer might not be surprised to see the ratio

$$\frac{p+1-a_p}{p+1+a_p}$$

show up; however, it is the square-root, contributed by RMT, that is the surprise.

The basic calculation to obtain this result involves a ratio of conjectures for

$$\sum_{\substack{d \equiv a \bmod p \\ d \le x}} L_{E_d}(1/2)^{-1/2};$$

the reason that one takes the -1/2 power here is due to the rightmost pole at $s = -1/2$ of the s'th moment of characteristic polynomials of matrices chosen randomly from $SO(2N)$ with respect to Haar measure. The description of this calculation and the compelling numerical evidence is in the paper [CKRS]. In this volume, the calculation is taken a step further in the paper of Conrey, Rubinstein, and Watkins where lower order terms for the moments are incorporated and lead to an even more precise evaluation of these ratios.

The conjectures about quadratic twists can be generalized to cubic twists in two different ways. One involves the frequency of rank 2 elliptic curves within the classical family $E_m := x^3 + y^3 = m$. See the interesting paper of Watkins to understand why it is precisely twice as likely that a number which is 2 mod 7 is a sum of two rational cubes compared with a number which is 3 mod 7.

The other way to do a cubic twist is to take a fixed elliptic curve E and a Dirichlet character χ of order 3 and consider the twisted L-function, $L_E(s, \chi) = \sum_{n=1}^{\infty} a_n \chi(n) n^{-s}$. David, Fearnley, and Kisilevsky [DFK] have shown, very surprisingly, that such twists vanish for about $x^{1/2}$ cubic twists of modulus $\leq x$, and have given precise conjectures, based on RMT, for the asymptotic frequency of this event. They also consider quintic twists (see their paper in this volume) and conclude that there are (barely!) infinitely many order five characters for which the twisted L-function vanishes at the central point. These predictions are based on calculations with random unitary matrices, whereas the previously mentioned conjectures arise from considering groups of orthogonal matrices.

It is interesting to begin with a weight 4 modular newform f, with integer Fourier coefficients, and similarly ask about vanishing of, say, quadratic twists of the associated L-function. In this case it is expected that there will be asymptotically $c_f x^{1/4} (\log x)^{b_f}$ vanishings at the central point of the quadratically twisted L-functions . The possible values of b_f have not been worked out here; however, if one restricts to prime discriminants, then the power on the log is expected to be $-5/8$ in both this case and the case of twists of elliptic curve L-functions. If one considers weight 6 or higher, it is expected that there will only be finitely many vanishings of quadratic twists of the associated L-functions. It is not clear whether one accumulates infinitely many vanishings if one considers all such weight 6 forms and all of their twists. There is an arithmetic significance to the vanishings of the twists of the weight 4 modular forms: it is related to the rank of an associated Chow group, about which we hope to say more at a later time.

In the twists mentioned in the cases above we only consider the twists for which there is a plus sign in the functional equation.

The numerical evidence for many of the above conjectures has been accumulated by a combination of people: Tornaria, Rodriguez-Villegas, Rosson, Mao, and Rubinstein. Much of it is based on an algorithm of Gross for finding the half-integral weight form, as a theta series involving ternary quadratic forms, whose Fourier coefficients yield the values of the twisted L-series at the central point. Prior to the February workshop, only a handful of such theta series were known. During that workshop, the first four people above worked out the obstacles to further progress and produced literally thousands of examples for Rubinstein who computed hundreds of millions of values for each; this provides a nice data bank for testing conjectures.

Matt Young has considered the situation of the "family of all elliptic

curves." Basically he parametrizes this family as $E_{A,B} : y^2 = x^3 + Ax + B$ and allows (A, B) to run over a rectangle. He is concerned not only with the distribution of ranks in this family, but also with statistics such as the 'one-level density' of the zeros. He considers other more exotic families as well, such as E_{A,B^2} which is forced to have rank at last one. Such families play a role in Iwaniec' approach to the Riemann Hypothesis.

All of the above discussion has been focused on rank two. The question of modelling rank 3 members of a family is much more difficult; in fact it is not at all satisfactorily addressed. In the case of quadratic twists, to conjecture the number of rank 2 curves the application of random matrix theory relies on a discretization arising from the beautiful formula, due in this form to Kohnen and Zagier:

$$L_{E_d}(1/2) = \kappa_E \frac{c_E(|d|)^2}{\sqrt{|d|}},$$

where $c_E(|d|)$ is an integer and $\kappa_E > 0$. In the case of rank 3, we consider the conjectural formula of Birch and Swinnerton-Dyer for the value of the derivative of an odd $L_{E_d}(s)$:

$$L'_{E_d}(1/2) = \frac{h_{E_d}|Sha_{E_d}|}{\sqrt{d}},$$

where h_{E_d} is the height of a generating point. (Change this to the formula of Gross-Zagier.) The problem is that we don't know what kind of discretization to give h_P. It could conceivably be as small as $\log|d|$ but statistically this does not seem to be the correct model. By the work of Snaith (in this volume), the right-most pole of the derivative of the sth moment of characteristic polynomials of odd orthogonal matrices occurs at $s = -3/2$. This might suggest, if one uses the discretization $(\log|d|)/\sqrt{|d|}$, that there are only about $x^{1/4}$ rank 3 curves among the family of twists with conductor smaller than x. However, Rubin and Silverberg give examples of E which have many more rank 3 quadratic twists, suggesting that this discretization is not correct. In examining the limited data we have for rank 3 twists, an interesting phenomenon seems to appear: it looks as though $L'_{E_d}(1/2)$ cannot be as small as $(\log|d|)/\sqrt{|d|}$. Is it possible that when Sha is small then the height of a generating point is big and vice-versa? This linkage does not seem unnatural if one compares for example to the situation of the class number of a real quadratic field. There one finds that the product of the regulator times the size of the class group is always about the size of the square root of the discriminant. However, this analogy may not be correct, since this involves L-functions at the edge of the critical strip whereas we are discussing values at the center. The paper of Conrey, Rubinstein, Snaith, and Watkins discusses the so-called 'Saturday night conjecture' about the possible sizes of this product. Much more data is needed to make an informed conclusion.

All of the above and more is contained in this volume. Other directions yet to be considered are odd weight modular forms, Siegel modular forms, and

Chow groups and we hope this collection of papers will attract new researchers to this field and inspire those well acquainted with it to explore further.

References

[1] J.B. Conrey, J.P. Keating, M. Rubinstein, N.C. Snaith, On the frequency of vanishing of quadratic twists of modular L-functions, Number theory for the Milennium I, 301–315, Editors: M. A. Bennett, B. C. Berndt, N. Boston NH. G. , Diamond, A. J. Hildebrand, W. Philipp, A. K. Peters Ltd, Natick, 2002.

[2] C. David, J. Fearnley and H. Kisilevsky, On the Vanishing of Twisted L-Functions of Elliptic Curves, *Experimental Mathematics*, 13 (2004), 185–198.

Elliptic curves, rank in families and random matrices

E. Kowalski

This survey paper contains two parts. The first one is a written version of a lecture given at the "Random Matrix Theory and L-functions" workshop organized at the Newton Institute in July 2004. This was meant as a very concrete and down to earth introduction to elliptic curves with some description of how random matrices become a tool for the (conjectural) understanding of the rank of Mordell-Weil groups by means of the Birch and Swinnerton-Dyer Conjecture; the reader already acquainted with the basics of the theory of elliptic curves can certainly skip it. The second part was originally the write-up of a lecture given for a workshop on the Birch and Swinnerton-Dyer Conjecture itself, in November 2003 at Princeton University, dealing with what is known and expected about the variation of the rank in families of elliptic curves. Thus it is also a natural continuation of the first part. In comparison with the original text and in accordance with the focus of the first part, more details about the input and confirmations of Random Matrix Theory have been added.

Acknowledgments. I would like to thank the organizers of both workshops for inviting me to gives these lectures, and H. Helfgott, C. Hall, C. Delaunay, S. Miller, M. Young and M. Rubinstein for helpful remarks, in particular for informing me of work in process of publication or in progress that I was unaware at the time of the talks. In fact, since this paper was written, a number of other relevant preprints have appeared; among these we mention [Sn], [Mil2], with no claim to exhaustivity!

Notation. We use synonymously the two notations $f(x) = O(g(x))$ and $f(x) \ll g(x)$ for $x \in X$, where X is some set on which both f and $g \geqslant 0$ are defined; it means that for some "implied" constant $C \geqslant 0$ (which may depend on further parameters), we have $|f(x)| \leqslant Cg(x)$ for all $x \in X$. On the other hand, we use $f = o(g)$ as $x \to x_0$, for some limit point x_0, to mean that the limit of f/g exists and is 0 as $x \to x_0$, and similarly $f \sim g$ for $x \to x_0$ means $f/g \to 1$ as $x \to x_0$.

1 A concrete introduction to elliptic curves

Before embarking on our journey, we refer in general to Silverman's book [AEC] for a very good and readable discussion of the topics covered here, with complete proofs for all but the most advanced. Each subsection will include ref-

erences to the parts of this book that corresponds, and other references if necessary.

1.1 Elliptic curves as algebraic curves, complex tori and the link between the two

Elliptic curves can be seen in a number of different ways. We will present the two most geometric. First, an *affine plane cubic curve* over the field $\mathbf{C}$ of complex numbers is simply the set of complex solutions $(x, y) \in \mathbf{C} \times \mathbf{C}$ of an equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.1}$$

(called a *general Weierstrass equation*), where a_1, a_2, a_3, a_4 and a_6 are arbitrary complex numbers. If all the a_i are rational numbers, the curve is said to be *defined over* $\mathbf{Q}$. It is those curves which are most relevant for number theory, and especially one is concerned with the basic diophantine question which is to find all rational solutions $(x, y) \in \mathbf{Q} \times \mathbf{Q}$ to the equation (1.1).

For many reasons, it is usually more convenient to present the equation (1.1) in homogeneous form

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{1.2}$$

(which defines a *projective cubic curve*) and look for triplets of solutions (X, Y, Z) in the projective plane $\mathbf{P}_2(\mathbf{C})$ instead of the place $\mathbf{C}^2$, which means looking for non-zero solutions $(X, Y, Z) \neq (0, 0, 0)$ and identifying two solutions (X, Y, Z) and $(\alpha X, \alpha Y, \alpha Z)$ for any non-zero $\alpha \in \mathbf{C}^\times$.

If in a triplet (X, Y, Z) satisfying (1.2) we have $Z \neq 0$, then we can replace (X, Y, Z) by the equivalent solution $(X/Z, Y/Z, 1)$ and this satisfies (1.2) if and only if the pair $(x, y) = (X/Z, Y/Z)$ satisfies the original equation (1.1). So the homogeneous solutions with $Z \neq 0$ are in one-to-one correspondence with the points on the affine cubic curve. However, if $Z = 0$, the equation (1.2) gives $X = 0$, so the solutions are $(0, Y, 0)$ with $Y \neq 0$ arbitrary. All those are in fact equivalent to a single solution $(0, 1, 0)$, which is called the *point at infinity*, often denote ∞. Note in particular that this point always has rational coordinates.

Plane cubic curves provide the first "picture" of elliptic curves, that as algebraic curves. However, there is a necessary condition imposed on an equation (1.1) before it is said to be the equation of an elliptic curve, namely it must define a smooth curve in $\mathbf{C} \times \mathbf{C}$. This means that the partial derivatives

$$2y + a_1x + a_3 \quad \text{and} \quad a_1y - 3x^2 - 2a_2x - a_4$$

must not have a common zero (x, y) which is also a point on the cubic curve. There is an explicit "numeric" criterion for this to hold (see [AEC, p. 46]); in the slightly simpler case where $a_1 = a_3 = 0$ (we will see that one can reduce to this case in most situations), the smoothness expresses simply that the cubic

polynomial $x^3+a_2x^2+a_4x+a_6$ has three distinct roots in $\mathbf{C}$, equivalently that the *discriminant* $\Delta = -16(4a_4^3+27a_6^2)$ is non-zero. Thus, this will be true for a "random" equation (1.1).

To summarize this definition: an elliptic curve, as an algebraic curve, is the set of projective solutions (X, Y, Z) to an equation (1.2) which defines a smooth curve.

Example 1.1. • The plane cubic curve with equation

$$y^2 = x^3$$

is not an elliptic curve: the point $(0,0)$ is a singular point (the curve looks like a "cusp" in the neighborhood of $(0,0)$).

• Similarly, the curve with equation

$$y^2 = x^3 + x^2$$

is not an elliptic curve; again $(0,0)$ is singular, and the curve looks like a node in the neighborhood of $(0,0)$.

• The curve with equation

$$y^2 = x^3 - x = x(x-1)(x+1)$$

is an elliptic curve, since the right-hand side has three distinct roots in $\mathbf{C}$. This curve is defined over $\mathbf{Q}$. It is often called the *congruent number* curve, for reasons we will explain below; it is also a so-called *CM curve*, and this terminology will also be explained.

• Let $\ell > 2$ be a prime number. *If* (a, b, c) were non-zero rationals such that $a^\ell + b^\ell = c^\ell$, then the cubic curve

$$y^2 = x(x-a^\ell)(x+b^\ell)$$

would be a very remarkable elliptic curve (defined over $\mathbf{Q}$), in fact so remarkable that it cannot possibly exist: this is the "highest level" summary of how Wiles proved Fermat's Great Theorem.

The other view of elliptic curves is more analytic in flavor, and identifies them with *complex tori*. Namely, let ω_1, ω_2 be non-zero complex numbers, with $\omega_1/\omega_2 \notin \mathbf{R}$. Let $\Lambda = \omega_1\mathbf{Z} \oplus \omega_2\mathbf{Z}$; this is an abelian subgroup of $\mathbf{C}$, and it generates $\mathbf{C}$ as an $\mathbf{R}$-vector space. Those two properties characterize the *lattices* in $\mathbf{C}$, and all of them are given as described.

Now consider the quotient group $X = \mathbf{C}/\Lambda$ which one views as a compact Riemann surface (it is compact because, for instance the compact set $\{a\omega_1 + b\omega_2 \mid (a,b) \in [0,1]\times[0,1]\}$ projects surjectively to X). Topologically, this is a torus, and as a group, this is $(\mathbf{R}/\mathbf{Z})^2$. Now the analytic definition of an elliptic curve is simply that it is one such quotient $\mathbf{C}/\Lambda$ for some lattice $\Lambda \subset \mathbf{C}$. We will now discuss how this definition and that as smooth plane cubic curve are

compatible. A small warning: although it is tempting to think so at first, taking ω_i with rational coordinates does not give the analogue of cubic curves defined over $\mathbf{Q}$! In fact, for a curve defined over $\mathbf{Q}$, the ratio ω_2/ω_1 is almost always transcendental, see e.g. [Ba, Ch. 6].

It is always natural to look for meromorphic functions defined on a Riemann surface (for instance, think that on a cubic curve we have two natural rational functions, $(x, y) \mapsto x$ and $(x, y) \mapsto y$ which are used to give the equation of the curve). Very concretely, this means we wish to consider meromorphic functions

$$f : \mathbf{C} \to \mathbf{C}$$

which are ω_1 and ω_2-periodic:

$$f(z + \omega_1) = f(z) \text{ and } f(z + \omega_2) = f(z).$$

Those f are called *elliptic functions*; this is where the history began in fact, since it was found, over a long period, that the arc-length on an ellipse can be expressed in terms of (inverses of) such functions (see [AEC, 168–170] for a sequence of exercises explaining this).

Now for a given Λ, one can construct an elliptic function $\wp$ which has a pole of order 2 at points of Λ and no other singularities, and satisfies the algebraic differential equation

$$\wp'^2 = 4\wp^3 - g_2\wp - g_3$$

for some g_2, $g_3 \in \mathbf{C}$. In fact, this is the Weierstrass $\wp$-function of Λ which is given explicitly by the series

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}} \Big(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\Big),$$

and g_2 and g_3 are the absolutely convergent series

$$g_2 = 60 \sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}} \frac{1}{\omega^4}, \quad g_3 = 140 \sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}} \frac{1}{\omega^6}.$$

Sending $z \mapsto (2\wp(z), \sqrt{2}\wp'(z))$ gives points on the plane cubic

$$y^2 = x^3 - g_2 x - 2g_3 \tag{1.3}$$

with $0 \mapsto \infty$ since $\wp$ has a pole at $z = 0$. One shows that this map is bijective, and that this cubic curve is smooth, hence is an elliptic curve "as plane curve". Moreover, one shows that all elliptic curves with $a_1 = a_3 = a_2 = 0$ arise in this manner, and also that simple changes of variables can bring any Weierstrass equation (1.2) to the form (1.3).

References: [AEC, III.1,VI]