Conference Board of the Mathematical Sciences

CBMS

Regional Conference Series in Mathematics

Number 101

Rational Points on Modular Elliptic Curves

Henri Darmon

American Mathematical Society
with support from the
National Science Foundation

Rational Points on Modular Elliptic Curves

This page intentionally left blank

http://dx.doi.org/10.1090/cbms/101

Conference Board of the Mathematical Sciences

CBMS

Regional Conference Series in Mathematics

Number 101

Rational Points on Modular Elliptic Curves

Henri Darmon

Published for the
Conference Board of the Mathematical Sciences
by the
American Mathematical Society
Providence, Rhode Island
with support from the
National Science Foundation

CBMS Conference on Modular Elliptic Curves held at
University of Central Florida
August 8–12, 2001

Partially supported by the National Science Foundation

2000 *Mathematics Subject Classification.* Primary 11G40;
Secondary 11F67, 11F85, 11G18, 11R37.

For additional information and updates on this book, visit
www.ams.org/bookpages/cbms-101

Library of Congress Cataloging-in-Publication Data

Darmon, Henri, 1965–
Rational points on modular elliptic curves /Henri Darmon.
p. cm. — (Regional conference series in mathematics, ISSN 0160-7642 ; no. 101)
Includes bibliographical references.
ISBN 0-8218-2868-1 (alk. paper)
1. Curves, Elliptic. 2. Curves, Modular. 3. Rational points (Geometry) I. Title. II. Series.

QA1 .R33 no. 101
QA567.2.E44
510 s—dc22
516.3′52 2003063735

---

10 9 8 7 6 5 4 3 2 1 09 08 07 06 05 04

A Galia et Maia

This page intentionally left blank

Contents

This page intentionally left blank

Preface

This monograph is based on an NSF-CBMS lecture series given by the author at the University of Central Florida in Orlando from August 8 to 12, 2001.

The goal of this lecture series was to survey some recent developments in the arithmetic of modular elliptic curves, with special emphasis on

(1) the Birch and Swinnerton-Dyer conjecture;
(2) the construction of rational points on modular elliptic curves;
(3) the crucial role played by modularity in shedding light on these two closely related issues.

The text is divided into three parts of roughly equal length.

The first consists of Chapters 1–3 and Chapter 10. The first three chapters introduce the background and prerequisites for what follows: elliptic curves, modular forms and the Shimura-Taniyama-Weil conjecture, complex multiplication, and the fundamental *Heegner point construction* whose study and generalisation is the main theme of the monograph. The notion of "Heegner system", which is spelled out in Chapter 3, is used in Chapter 10 to prove Kolyvagin's theorem relating Heegner points to the arithmetic of elliptic curves, giving strong evidence for the Birch and Swinnerton-Dyer conjecture for elliptic curves of analytic rank at most one. While more advanced than Chapters 1–3, Chapter 10 is independent of the material in Chapters 4–9 and could be read immediately after Chapter 3.

Chapters 4–6 introduce variants of modular parametrisations in which modular curves are replaced by Shimura curves attached to certain indefinite quaternion algebras. A study of these parametrisations reveals an important new structure: the rigid analytic uniformisation of Shimura curves discovered by Čerednik and Drinfeld, giving rise to p-adic uniformisations of modular elliptic curves by discrete arithmetic subgroups of $\mathbf{SL}_2(\mathbb{Q}_p)$ arising from definite quaternion algebras.

The main new contributions of this monograph are contained in Chapters 7–9. These Chapters give an overview of the author's attempts to extend the theory of Heegner points and complex multiplication to certain situations where the base field is not a CM field. The notions of rigid analysis developed in Chapters 5 and 6 play a key role in suggesting a p-adic variant of the theories of Chapters 7 and 8. This leads, in Chapter 9, to a conjectural construction of points on a modular elliptic curve over $\mathbb{Q}$ defined over ring class fields of a *real* quadratic field, which are expected to behave much like classical Heegner points attached to an imaginary quadratic field.

The reader is cautioned that many proofs give only the main ideas; details have often been left out or relegated to exercises, retaining (for better or for worse) the flavour of the original lecture series. Of necessity, a number of important

topics had to be omitted or inadequately touched upon, for lack of time. The material covered here would be suitable for a 10-hour to 15-hour mini-course, or, with extra background material, for a one-semester or even a year-long seminar aimed at graduate students.

A selection of exercises is given at the end of most chapters. Many of these consist in working out the details of arguments sketched in the text. It is hoped that readers encountering this material for the first time will find the exercises helpful, while more sophisticated readers may elect to skip them without loss of continuity.

Some of the ideas discussed in this monograph have their roots in the author's collaboration with Massimo Bertolini over the years. Exchanges with Samit Dasgupta, Peter Green, Adrian Iovita and Adam Logan have also helped in forming and solidifying key insights. The author thanks Peter Hilton and Heath Martin of the University of Central Florida for the marvelous job they did in running the NSF-CBMS conference on which this monograph is based, as well as the participants for their many stimulating comments and suggestions. A rough version of this text formed the basis for a graduate seminar at McGill University in the 2002–2003 academic year, and at Priceton University in the Fall of 2003. The participants of the McGill seminar—Hugo Chapdelaine, Samit Dasgupta, Antoine Gournay, and Matt Greenberg—pointed out a number of mistakes in earlier versions. I am specially grateful to Pete Clark and Claude Levesque for their detailed proofreading of this manuscript which led to a large number of corrections and improvements. Needless to say, the imperfections and inaccuracies which remain are to be blamed on the author alone! Finally, it is a great pleasure to acknowledge my colleagues at CICMA, and NSERC, whose material support, in particular through the granting of a Steacie Fellowship, has greatly facilitated the writing of this monograph.

Henri Darmon
Montreal 2003

over $\mathbb{Q}$, and that $\mathrm{Gal}(L_s/\mathbb{Q})$ is identified with the semi-direct product

$$\mathrm{Gal}(L_s/\mathbb{Q}) = E_p \rtimes \mathrm{Gal}(L/\mathbb{Q}),$$

where the quotient $\mathrm{Gal}(L/\mathbb{Q})$ acts on the abelian normal subgroup E_p of $\mathrm{Gal}(L_s/\mathbb{Q})$ by the rule

$$(\zeta, \tau^j, T)(v) = \delta^j \bar{T} v.$$

(Here $\bar{T}$ denotes the natural image of T in $\mathrm{Aut}(E_p)$.)

(f) Show that the group $\mathrm{Gal}(L_s/\mathbb{Q})$ contains an element of the form $(v, 1, \tau, T)$, where the automorphism T is as in (d), and the vector $v \in E_p$ is non-zero and belongs to the δ-eigenspace for $\bar{T}$.

(g) Let $\ell \nmid N$ be a rational prime which is unramified in $L_s/\mathbb{Q}$ and satisfies

$$\mathrm{Frob}_\ell(L_s/\mathbb{Q}) = (v, 1, \tau, T).$$

Show that ℓ is a Kolyvagin prime, and that, if λ is the (unique) prime of K above ℓ, we have $s_\lambda \neq 0$. Conclude that there exist infinitely many Kolyvagin primes ℓ such that $\partial_\lambda(s) = 0$ and $s_\lambda \neq 0$.

(h) Let H be any finite-dimensional subspace of $H^1(K, E_p)$. Using (g), show that there is a finite set S of Kolyvagin primes with the property that the natural map induced by restriction

$$H \longrightarrow \bigoplus_v H^1(K_v, E_p)$$

is injective. Conclude Proposition 10.18.

(i) Prove Proposition 10.23.

(5) Show that, if ℓ is a Kolyvagin prime with respect to (E, K, p), then the p-Sylow subgroup of $E(\mathbb{F}_{\ell^2})$ is isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Conclude that the map η_ℓ obtained by composing the maps in the sequence (10.11) is an isomorphism.

(6) Following the notations in the proof of Proposition 10.21, show that:

$$\tau D_\ell = -D_\ell \tau \pmod{n_\ell}, \quad \tau D_{\ell_1} D_{\ell_2} = D_{\ell_1} D_{\ell_2} \tau \pmod{\gcd(n_{\ell_1}, n_{\ell_2})}.$$

(In particular, these identities hold modulo p^2.)

(7) Give the details of the construction of the cohomology classes $\kappa(\ell_1 \ell_2)$ depending on two Kolyvagin primes, and prove the properties asserted in Proposition 10.22.

Bibliography

[AL70] A.O.L. Atkin and J. Lehner. *Hecke operators on* $\Gamma_0(m)$. Math. Ann. **185** (1970) 134–160.

[BCDT01] C. Breuil, B. Conrad, F. Diamond, and R. Taylor. *On the modularity of elliptic curves over* $\mathbb{Q}$*: wild 3-adic exercises.* J. Amer. Math. Soc. **14** (2001), no. 4, 843–939.

[BC92] J-F. Boutot and H. Carayol. *Uniformisation p-adique des courbes de Shimura: les théorèmes de Cerednik et de Drinfeld.* Courbes modulaires et courbes de Shimura (Orsay, 1987/1988). Astérisque No. 196-197 (1991) 45–158.

[BD96] M. Bertolini and H. Darmon. *Heegner points on Mumford-Tate curves.* Invent. Math **126** (1996) 413–456.

[BD97] M. Bertolini and H. Darmon. *A rigid-analytic Gross-Zagier formula and arithmetic applications.* Annals of Math **146** (1997) 111-147.

[BD98] M. Bertolini and H. Darmon. *Heegner points, p-adic L-functions, and the Cerednik-Drinfeld uniformisation.* Invent. Math. **131** (1998) 453–491.

[BD99] M. Bertolini and H. Darmon. *p-adic periods, p-adic L-functions and the p-adic uniformisation of Shimura curves.* Duke Math. J. **98** (1999), no. 2, 305–334.

[BD01] M. Bertolini and H. Darmon. *The p-adic L-functions of modular elliptic curves.* In Mathematics Unlimited—2001 and Beyond, 109–170, Springer-Verlag, Berlin, 2001.

[BD03] M. Bertolini and H. Darmon. *Iwasawa's main conjecture for elliptic curves in the anticyclotomic setting.* Annals of Mathematics, to appear.

[BDIS02] M. Bertolini, H. Darmon, A. Iovita, and M. Spiess. *Teitelbaum's conjecture in the anticyclotomic setting.* American Journal of Mathematics **124** (2002) 411-449.

[BDG03] M. Bertolini, H. Darmon, and P. Green. *Periods and points attached to quadratic algebras.* To appear in the Proceedings of an MSRI workshop on special values of Rankin L-series. H. Darmon and S. Zhang, eds.

[BFH90] D. Bump, S. Friedberg and J. Hoffstein. *Eisenstein series on the metaplectic group and nonvanishing theorems for automorphic L-functions and their derivatives.* Ann. of Math. (2) **131** (1990), no. 1, 53–127.

[Br94] K.S. Brown. Cohomology of groups. Corrected reprint of the 1982 original. Graduate Texts in Mathematics **87** Springer-Verlag, New York, 1994.

[BSD63] B.J. Birch and H.P.F. Swinnerton-Dyer. Notes on elliptic curves. I. J. Reine Angew. Math. **212** (1963) 7–25.

[BSD65] B.J. Birch and H.P.F. Swinnerton-Dyer. Notes on elliptic curves. II. J. Reine Angew. Math. **218** (1965) 79–108.

[Bu97] D. Bump. Automorphic forms and representations. Cambridge Studies in Advanced Mathematics, **55**. Cambridge University Press, Cambridge, 1997.

[Car86] H. Carayol. *Sur la mauvaise réduction des courbes de Shimura.* Compositio Math. **59** (1986), no. 2, 151–230.

[Car91] H. Carayol. *Formes modulaires et représentations galoisiennes à valeurs dans un anneau local complet.* In p-adic monodromy and the Birch and Swinnerton-Dyer conjecture (Boston, MA, 1991), 213–237, Contemp. Math., 165, Amer. Math. Soc., Providence, RI, 1994.

[Cas91] J.W.S. Cassels. Lectures on elliptic curves. London Mathematical Society Student Texts, **24**. Cambridge University Press, Cambridge, 1991.

[CDT99] B. Conrad, F. Diamond, and R. Taylor. *Modularity of certain potentially Barsotti-Tate Galois representations.* J. Amer. Math. Soc. **12** (1999), no. 2, 521–567.

[Ce76] I.V. Čerednik. *Uniformization of algebraic curves by discrete arithmetic subgroups of* $\mathrm{PGL}_2(k_w)$ *with compact quotient spaces.* Mat. Sb. (N.S.) 100(142) (1976), no. 1, 59–88.

[CF67] Algebraic number theory. Proceedings of an instructional conference organized by the London Mathematical Society. Edited by J. W. S. Cassels and A. Fröhlich. Academic Press, London; Thompson Book Co., Inc., Washington, D.C. 1967.

[Cl03] P. Clark. Rational points on Atkin-Lehner quotients of Shimura curves. Harvard PhD Thesis, 2003.

[Con] K. Conrad. *On a conjecture of Birch and Swinnerton-Dyer: Partial Euler products on the critical line.* Canadian Journal of Mathematics, to appear.

[Cor02] C. Cornut. *Mazur's conjecture on higher Heegner points.* Invent. Math. **148** (2002), no. 3, 495–523.

[Cox89] D.A. Cox. Primes of the form $x^2 + ny^2$. Fermat, class field theory and complex multiplication. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1989.

[Cr97] J.E. Cremona. Algorithms for modular elliptic curves. Second edition. Cambridge University Press, Cambridge, 1997.

[Da92] H. Darmon. *Heegner points, Heegner cycles, and congruences.* In "Elliptic curves and related topics", CRM proceedings and lecture notes vol. **4**, H. Kisilevsky and M. Ram Murty eds. (1992) 45–60.

[Da96] H. Darmon. *Stark-Heegner points over real quadratic fields.* Number theory (Tiruchirapalli, 1996), 41–69, Contemp. Math., **210**, Amer. Math. Soc., Providence, RI, 1998.

[Da01] H. Darmon. *Integration on $\mathcal{H}_p \times \mathcal{H}$ and arithmetic applications.* Annals of Mathematics **154** (2001) 589–639.

[Da02] H. Darmon. *Review of the book "Euler Systems" by Karl Rubin.* Bull. Amer. Math. Soc. **39** (2002) 407–414.

[Da03] H. Darmon. *Heegner points and elliptic curves of large rank over function fields.* To appear in the proceedings of an MSRI Workshop on Special Values of Rankin L-series. H. Darmon and S. Zhang, eds.

[DDT95] H. Darmon, F. Diamond, and R. Taylor. *Fermat's last theorem.* In Current developments in mathematics, 1995 (Cambridge, MA), 1–154, Internat. Press, Cambridge, MA, 1994. Reprinted in: Elliptic curves, modular forms & Fermat's last theorem (Hong Kong, 1993), 2–140, Internat. Press, Cambridge, MA, 1997.

[DG01] H. Darmon and P. Green. *Elliptic curves and class fields of real quadratic fields: algorithms and evidence.* Journal of Experimental Mathematics **11:1** (2002) 37-55.

[DL03] H. Darmon and A. Logan. *Periods of Hilbert modular forms and rational points on elliptic curves.* International Mathematics Research Notices, submitted.

[Di96] F. Diamond. *On deformation rings and Hecke rings.* Ann. of Math. (2) **144** (1996) 137–166.

[DI95] F. Diamond and J. Im. *Modular forms and modular curves.* In Seminar on Fermat's Last Theorem (Toronto, ON, 1993–1994), 39–133, CMS Conf. Proc., 17, Amer. Math. Soc., Providence, RI, 1995.

[Dr76] V.G. Drinfeld. *Coverings of p-adic symmetric domains.* Funkcional. Anal. i Prilozen. **10** (1976), no. 2, 29–40.

[DS95] E. de Shalit, *p-adic periods and modular symbols of elliptic curves of prime conductor.* Invent. Math. **121** (1995), no. 2, 225–255.

[Ed89] B. Edixhoven, *On the Manin constants of modular elliptic curves.* Arithmetic algebraic geometry (Texel, 1989), 25–39, Progr. Math., **89**, Birkhäuser Boston, Boston, MA, 1991.

[EGM98] J. Elstrodt, F. Grunewald, and J. Mennicke. Groups acting on hyperbolic space. Harmonic analysis and number theory. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 1998.

[Frei90] E. Freitag. Hilbert modular forms. Springer-Verlag, Berlin, 1990.

[Gar90] P.B. Garrett. Holomorphic Hilbert modular forms. The Wadsworth & Brooks/Cole Mathematics Series. Wadsworth & Brooks/Cole Advanced Books & Software, Pacific Grove, CA, 1990.

[Gel75] S.S. Gelbart. Automorphic forms on adele groups. Annals of Mathematics Studies, No. 83. Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1975.

[GKZ87] B. Gross, W. Kohnen and D. Zagier. *Heegner points and derivatives of L-series. II.* Math. Ann. **278** (1987), no. 1-4, 497–562.

[Go] D. Goldfeld. *Sur les produits partiels eulériens attachés aux courbes elliptiques.* C. R. Acad. Sci. Paris Sr. I Math. **294** (1982), no. 14, 471–474.

[Gr84] B.H. Gross. *Heegner points on $X_0(N)$.* In Modular forms (Durham, 1983), 87–105, Ellis Horwood Ser. Math. Appl.: Statist. Oper. Res., Horwood, Chichester, 1984.

[Gr87] B.H. Gross, *Heights and the special values of L-series.* In Number theory (Montreal, Que., 1985), 115–187, CMS Conf. Proc., **7**, Amer. Math. Soc., Providence, RI, 1987.

[Gr89] B.H. Gross. *Kolyvagin's work on modular elliptic curves.* In L-functions and arithmetic (Durham, 1989), 235–256, London Math. Soc. Lecture Note Ser., 153, Cambridge Univ. Press, Cambridge, 1991.

[GvdP80] L. Gerritzen and M. van der Put. Schottky groups and Mumford curves. Lecture Notes in Mathematics, **817**. Springer, Berlin, 1980.

[GS93] R. Greenberg and G. Stevens. *p-adic L-functions and p-adic periods of modular forms.* Invent. Math. **111** (1993), no. 2, 407–447.

[GZ84] B.H. Gross and D.B. Zagier. *Heegner points and derivatives of L-series.* Invent. Math. **84** (1986), no. 2, 225–320.

[Ha75] G. Harder. *On the cohomology of discrete arithmetically defined groups.* In Discrete subgroups of Lie groups and applications to moduli (Internat. Colloq., Bombay, 1973) 129–160. Oxford Univ. Press, Bombay, 1975.

[HST93] M. Harris, D. Soudry, and R. Taylor. *l-adic representations associated to modular forms over imaginary quadratic fields. I. Lifting to* $\mathrm{GSp}_4(Q)$. Invent. Math. **112** (1993), no. 2, 377–411.

[Hu87] D. Husemoller. Elliptic curves. With an appendix by Ruth Lawrence. Graduate Texts in Mathematics, **111**. Springer-Verlag, New York, 1987.

[Ih68] Y. Ihara. *On congruence monodromy problems.* Vol. 1. Lecture Notes, No. 1 Department of Mathematics, University of Tokyo, Tokyo 1968.

[Ih79] Y. Ihara. *Congruence relations and Shimura curves.* Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2, pp. 291–311, Proc. Sympos. Pure Math., XXXIII, Amer. Math. Soc., Providence, R.I., 1979.

[Ja72] H. Jacquet. *Automorphic forms on* GL(2). *Part II.* Lecture Notes in Mathematics **278**. Springer-Verlag, Berlin-New York, 1972.

[JL70] H. Jacquet and R.P. Langlands. Automorphic forms on GL(2). Lecture Notes in Mathematics **114**. Springer-Verlag, Berlin-New York, 1970.

[Ka92] S. Katok. Fuchsian groups. Chicago Lectures in Mathematics. University of Chicago Press, Chicago, IL, 1992.

[Kl91] C. Klingenberg. *On p-adic L-functions of Mumford curves.* In p-adic monodromy and the Birch and Swinnerton-Dyer conjecture (Boston, MA, 1991), 277–315, Contemp. Math., **165**, Amer. Math. Soc., Providence, RI, 1994.

[Kn92] A.W. Knapp. Elliptic curves. Mathematical Notes, 40. Princeton University Press, Princeton, NJ, 1992.

[Kob93] N. Koblitz. Introduction to elliptic curves and modular forms. Second edition. Graduate Texts in Mathematics **97**. Springer-Verlag, New York, 1993.

[Kol88] V.A. Kolyvagin. *Finiteness of $E(Q)$ and $Ш(E,\mathbb{Q})$ for a subclass of Weil curves.* (Russian) Izv. Akad. Nauk SSSR Ser. Mat. **52** (1988), no. 3, 522–540, 670–671; translation in Math. USSR-Izv. **32** (1989), no. 3, 523–541.

[Kol89] V.A. Kolyvagin. *The Mordell-Weil and Shafarevich-Tate groups for Weil elliptic curves.* (Russian) Izv. Akad. Nauk SSSR Ser. Mat. **52** (1988), no. 6, 1154–1180, 1327; translation in Math. USSR-Izv. **33** (1989), no. 3, 473–499.

[Kol90] V.A. Kolyvagin. *Euler systems.* In The Grothendieck Festschrift, Vol. II, 435–483, Progr. Math. **87**, Birkhäuser Boston, Boston, MA, 1990.

[Man72] Ju.I. Manin. Parabolic points and zeta functions of modular curves. (Russian) Izv. Akad. Nauk SSSR Ser. Mat. **36** (1972), 19–66.

[Men67] J. Mennicke, *On Ihara's modular group.* Invent. Math. **4** (1967) 202–228.

[Mes91] J.-F. Mestre. *Courbes elliptiques de rang ≥ 12 sur $Q(t)$.* C. R. Acad. Sci. Paris Sr. I Math **313** (1991), no. 4, 171–174.

[Mi86] J.S. Milne. Arithmetic duality theorems. Perspectives in Mathematics, 1. Academic Press, Inc., Boston, MA, 1986.

[MM91] M.R. Murty and V.K. Murty. *Mean values of derivatives of modular L-series.* Ann. of Math. (2) **133** (1991), no. 3, 447–475.

[MM97] M.R. Murty and V.K. Murty. *Non-vanishing of L-functions and applications.* Progress in Mathematics **157**. Birkhäuser Verlag, Basel, 1997.

[MTT] B. Mazur, J. Tate, and J. Teitelbaum. *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer.* Invent. Math. **84** (1986), no. 1, 1–48.

[MSw-D74] B. Mazur and P. Swinnerton-Dyer. *Arithmetic of Weil curves.* Invent. Math. **25** (1974) 1–61.

[MS78] Y. Matsushima and G. Shimura. *On the cohomology groups attached to certain vector-valued differential forms on the product of upper half planes.* Ann. of Math. (2) **78** (1963) 417–449.

[Mu] V.K. Murty. Introduction to abelian varieties. CRM Monograph Series, 3. American Mathematical Society, Providence, RI, 1993.

[Od82] T. Oda. Periods of Hilbert modular surfaces. Progress in Mathematics **19**. Birkhäuser, Boston, Mass., 1982.

[Og69] A. Ogg. Modular forms and Dirichlet series. W. A. Benjamin, Inc., New York-Amsterdam 1969.

[Ri94] K.A. Ribet. *Fields of definition of abelian varieties with real multiplication.* In Arithmetic geometry (Tempe, AZ, 1993), 107–118, Contemp. Math., 174, Amer. Math. Soc., Providence, RI, 1994.

[Ro96] D.E. Rohrlich. *Galois theory, elliptic curves, and root numbers.* Compositio Math. **100** (1996), no. 3, 311–349.

[Ru00] K. Rubin. Euler systems. Annals of Mathematics Studies **147**. Hermann Weyl Lectures. The Institute for Advanced Study. Princeton University Press, Princeton, NJ, 2000.

[Sch84] P. Schneider. *Rigid-analytic L-transforms.* Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), 216–230, Lecture Notes in Math **1068**, Springer, Berlin, 1984.

[Se67] J.-P. Serre. *Complex multiplication.* Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965) 292–296, Thompson, Washington, D.C.

[Se70] J.-P. Serre. *Le problème des groupes de congruence pour* $\mathbf{SL}_2$. Ann. of Math. (2) **92** (1970) 489–527.

[Se71] J.-P. Serre. *Cohomologie des groupes discrets.* In Prospects in mathematics (Proc. Sympos., Princeton Univ., Princeton, N.J., 1970), 77–169. Ann. of Math. Studies, No. 70, Princeton Univ. Press, Princeton, N.J., 1971.

[Se72] J.-P. Serre. *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques.* Invent. Math. **15** (1972), no. 4, 259–331.

[Se80] J.-P. Serre. Trees. Translated from the French by John Stillwell. Springer-Verlag, Berlin-New York, 1980.

[Sh64] G. Shimura, *Class-fields and automorphic functions.* Ann. of Math. (2) **80** (1964) 444–463.

[Sh67] G. Shimura, *Construction of class fields and zeta functions of algebraic curves.* Ann. of Math. (2) **85** (1967) 58–159.

[Sh71] G. Shimura. Introduction to the arithmetic theory of automorphic functions. Reprint of the 1971 original. Publications of the Mathematical Society of Japan, 11. Kanô Memorial Lectures, 1. Princeton University Press, Princeton, NJ, 1994.

[Sh86] G. Shimura, *Algebraic number fields and symplectic discontinuous groups.* Ann. of Math. (2) **86** (1967) 503–592.

[Si86] J.H. Silverman. The arithmetic of elliptic curves. Corrected reprint of the 1986 original. Graduate Texts in Mathematics **106**. Springer-Verlag, New York, 1986.

[Si94] J.H. Silverman. Advanced topics in the arithmetic of elliptic curves. Graduate Texts in Mathematics **151**. Springer-Verlag, New York, 1994.

[Sta87] H.M. Stark. *Modular forms and related objects.* In Number theory (Montreal, Que., 1985), 421–455, CMS Conf. Proc., 7, Amer. Math. Soc., Providence, RI, 1987.

[ST92] J.H. Silverman and J. Tate. *Rational points on elliptic curves.* Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.

[Ta62] J. Tate. *Duality theorems in Galois cohomology over number fields.* 1963 Proc. Internat. Congr. Mathematicians (Stockholm, 1962) 288–295, Inst. Mittag-Leffler, Djursholm.

[Ta72] J. Tate. *Algorithm for determining the type of a singular fiber in an elliptic pencil.* In Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), 33–52. Lecture Notes in Math. **476**, Springer, Berlin, 1975.

[Ta74] J. Tate. *The arithmetic of elliptic curves.* Invent. Math. **23** (1974) 179–206.

[Te90] J.T. Teitelbaum. *Values of p-adic L-functions and a p-adic Poisson kernel.* Invent. Math. **101** (1990), no. 2, 395–410.

[TS67] J.T. Tate and I.R. Šafarevič. *The rank of elliptic curves.* (Russian) Dokl. Akad. Nauk SSSR **175** (1967) 770–773.

[T94] R. Taylor. *l-adic representations associated to modular forms over imaginary quadratic fields. II.* Invent. Math. **116** (1994), no. 1-3, 619–643.

[TW95] R. Taylor and A. Wiles. *Ring-theoretic properties of certain Hecke algebras.* Ann. of Math. (2) **141** (1995), no. 3, 553–572.

[Ul] D. Ulmer. *Elliptic curves with large rank over function fields.* Ann. of Math. (2) **155** (2002), no. 1, 295–315.

[Vi80] M.-F. Vignéras. Arithmétique des algèbres de quaternions. Lecture Notes in Mathematics **800**. Springer, Berlin, 1980.

[Va02] V. Vatsal. *Uniform distribution of Heegner points.* Invent. Math. **148** (2002), no. 1, 1–46.

[Wa85] J.-L. Waldspurger. *Sur les valeurs de certaines fonctions L automorphes en leur centre de symétrie.* Compositio Math. **54** (1985), no. 2, 173–242.

[Wi88] A. Wiles. *On ordinary λ-adic representations associated to modular forms.* Invent. Math. **94** (1988), no. 3, 529–573.

[Wi95] A. Wiles. *Modular elliptic curves and Fermat's last theorem.* Ann. of Math. (2) **141** (1995), no. 3, 443–551.

[Wi00] A. Wiles. *The Birch and Swinnerton-Dyer Conjecture*, Clay Mathematics Institute Web Site, http://www.claymath.org/prizeproblems/birchsd.pdf.

[Za85] D. Zagier. *Modular points, modular curves, modular surfaces and modular forms.* Workshop Bonn 1984 (Bonn, 1984), 225–248, Lecture Notes in Math. **1111**, Springer, Berlin, 1985.

[Zh01a] S. Zhang. *Heights of Heegner points on Shimura curves.* Ann. of Math. (2) **153** (2001), no. 1, 27–147.

[Zh01b] S. Zhang. *Gross-Zagier formula for* GL_2. Asian J. Math. **5** (2001), no. 2, 183–290.

This page intentionally left blank

Titles in This Series

101 **Henri Darmon,** Rational points on modular elliptic curves, 2004

100 **Alexander Volberg,** Calderón-Zygmund capacities and operators on nonhomogeneous spaces, 2003

99 **Alain Lascoux,** Symmetric functions and combinatorial operators on polynomials, 2003

98 **Alexander Varchenko,** Special functions, KZ type equations, and representation theory, 2003

97 **Bernd Sturmfels,** Solving systems of polynomial equations, 2002

96 **Niky Kamran,** Selected topics in the geometrical study of differential equations, 2002

95 **Benjamin Weiss,** Single orbit dynamics, 2000

94 **David J. Saltman,** Lectures on division algebras, 1999

93 **Goro Shimura,** Euler products and Eisenstein series, 1997

92 **Fan R. K. Chung,** Spectral graph theory, 1997

91 **J. P. May et al.,** Equivariant homotopy and cohomology theory, dedicated to the memory of Robert J. Piacenza, 1996

90 **John Roe,** Index theory, coarse geometry, and topology of manifolds, 1996

89 **Clifford Henry Taubes,** Metrics, connections and gluing theorems, 1996

88 **Craig Huneke,** Tight closure and its applications, 1996

87 **John Erik Fornæss,** Dynamics in several complex variables, 1996

86 **Sorin Popa,** Classification of subfactors and their endomorphisms, 1995

85 **Michio Jimbo and Tetsuji Miwa,** Algebraic analysis of solvable lattice models, 1994

84 **Hugh L. Montgomery,** Ten lectures on the interface between analytic number theory and harmonic analysis, 1994

83 **Carlos E. Kenig,** Harmonic analysis techniques for second order elliptic boundary value problems, 1994

82 **Susan Montgomery,** Hopf algebras and their actions on rings, 1993

81 **Steven G. Krantz,** Geometric analysis and function spaces, 1993

80 **Vaughan F. R. Jones,** Subfactors and knots, 1991

79 **Michael Frazier, Björn Jawerth, and Guido Weiss,** Littlewood-Paley theory and the study of function spaces, 1991

78 **Edward Formanek,** The polynomial identities and variants of $n \times n$ matrices, 1991

77 **Michael Christ,** Lectures on singular integral operators, 1990

76 **Klaus Schmidt,** Algebraic ideas in ergodic theory, 1990

75 **F. Thomas Farrell and L. Edwin Jones,** Classical aspherical manifolds, 1990

74 **Lawrence C. Evans,** Weak convergence methods for nonlinear partial differential equations, 1990

73 **Walter A. Strauss,** Nonlinear wave equations, 1989

72 **Peter Orlik,** Introduction to arrangements, 1989

71 **Harry Dym,** J contractive matrix functions, reproducing kernel Hilbert spaces and interpolation, 1989

70 **Richard F. Gundy,** Some topics in probability and analysis, 1989

69 **Frank D. Grosshans, Gian-Carlo Rota, and Joel A. Stein,** Invariant theory and superalgebras, 1987

68 **J. William Helton, Joseph A. Ball, Charles R. Johnson, and John N. Palmer,** Operator theory, analytic functions, matrices, and electrical engineering, 1987

67 **Harald Upmeier,** Jordan algebras in analysis, operator theory, and quantum mechanics, 1987

66 **G. Andrews,** q-Series: Their development and application in analysis, number theory, combinatorics, physics and computer algebra, 1986

65 **Paul H. Rabinowitz,** Minimax methods in critical point theory with applications to differential equations, 1986

64 **Donald S. Passman,** Group rings, crossed products and Galois theory, 1986

63 **Walter Rudin,** New constructions of functions holomorphic in the unit ball of C^n, 1986

62 **Béla Bollobás,** Extremal graph theory with emphasis on probabilistic methods, 1986

61 **Mogens Flensted-Jensen,** Analysis on non-Riemannian symmetric spaces, 1986

60 **Gilles Pisier,** Factorization of linear operators and geometry of Banach spaces, 1986

59 **Roger Howe and Allen Moy,** Harish-Chandra homomorphisms for $\mathfrak{p}$-adic groups, 1985

58 **H. Blaine Lawson, Jr.,** The theory of gauge fields in four dimensions, 1985

57 **Jerry L. Kazdan,** Prescribing the curvature of a Riemannian manifold, 1985

56 **Hari Bercovici, Ciprian Foiaş, and Carl Pearcy,** Dual algebras with applications to invariant subspaces and dilation theory, 1985

55 **William Arveson,** Ten lectures on operator algebras, 1984

54 **William Fulton,** Introduction to intersection theory in algebraic geometry, 1984

53 **Wilhelm Klingenberg,** Closed geodesics on Riemannian manifolds, 1983

52 **Tsit-Yuen Lam,** Orderings, valuations and quadratic forms, 1983

51 **Masamichi Takesaki,** Structure of factors and automorphism groups, 1983

50 **James Eells and Luc Lemaire,** Selected topics in harmonic maps, 1983

49 **John M. Franks,** Homology and dynamical systems, 1982

48 **W. Stephen Wilson,** Brown-Peterson homology: an introduction and sampler, 1982

47 **Jack K. Hale,** Topics in dynamic bifurcation theory, 1981

46 **Edward G. Effros,** Dimensions and C^*-algebras, 1981

45 **Ronald L. Graham,** Rudiments of Ramsey theory, 1981

44 **Phillip A. Griffiths,** An introduction to the theory of special divisors on algebraic curves, 1980

43 **William Jaco,** Lectures on three-manifold topology, 1980

42 **Jean Dieudonné,** Special functions and linear representations of Lie groups, 1980

41 **D. J. Newman,** Approximation with rational functions, 1979

40 **Jean Mawhin,** Topological degree methods in nonlinear boundary value problems, 1979

39 **George Lusztig,** Representations of finite Chevalley groups, 1978

38 **Charles Conley,** Isolated invariant sets and the Morse index, 1978

37 **Masayoshi Nagata,** Polynomial rings and affine spaces, 1978

36 **Carl M. Pearcy,** Some recent developments in operator theory, 1978

35 **R. Bowen,** On Axiom A diffeomorphisms, 1978

34 **L. Auslander,** Lecture notes on nil-theta functions, 1977

33 **G. Glauberman,** Factorizations in local subgroups of finite groups, 1977

32 **W. M. Schmidt,** Small fractional parts of polynomials, 1977

31 **R. R. Coifman and G. Weiss,** Transference methods in analysis, 1977

30 **A. Pełczyński,** Banach spaces of analytic functions and absolutely summing operators, 1977

29 **A. Weinstein,** Lectures on symplectic manifolds, 1977

28 **T. A. Chapman,** Lectures on Hilbert cube manifolds, 1976

27 **H. Blaine Lawson, Jr.,** The quantitative theory of foliations, 1977

The book surveys some recent developments in the arithmetic of modular elliptic curves. It places a special emphasis on the construction of rational points on elliptic curves, the Birch and Swinnerton-Dyer conjecture, and the crucial role played by modularity in shedding light on these two closely related issues.

The main theme of the book is the theory of complex multiplication, Heegner points, and some conjectural variants. The first three chapters introduce the background and prerequisites: elliptic curves, modular forms and the Shimura-Taniyama-Weil conjecture, complex multiplication and the Heegner point construction. The next three chapters introduce variants of modular parametrizations in which modular curves are replaced by Shimura curves attached to certain indefinite quaternion algebras. The main new contributions are found in Chapters 7–9, which survey the author's attempts to extend the theory of Heegner points and complex multiplication to situations where the base field is not a CM field. Chapter 10 explains the proof of Kolyvagin's theorem, which relates Heegner points to the arithmetic of elliptic curves and leads to the so-far best evidence for the Birch and Swinnerton-Dyer conjecture.

ISBN 0-8218-2868-1

9 780821 828687

CBMS/101