Lecture Notes in Mathematics

M. L. Brown

Heegner Modules and Elliptic Curves

1849

Springer

M. L. Brown

Heegner Modules and Elliptic Curves

Springer

Author

Martin L. Brown

Institut Fourier
BP 74
38402 Saint-Martin d'Hères
France

e-mail: Martin.Brown@ujf-grenoble.fr

Library of Congress Control Number: 2004107464

Mathematics Subject Classification (2000):
11F52, 11G05, 11G09, 11G15, 11G40, 11R58, 14F20, 14G10, 14H52, 14J27, 14K22

ISSN 0075-8434
ISBN 3-540-22290-1 Springer-Verlag Berlin Heidelberg New York
DOI: 10.1007/b98488

Springer is a part of Springer Science + Business Media
springeronline.com

Printed in Germany

Typesetting: Camera-ready TEX output by the authors

41/3142/du - 543210 - Printed on acid-free paper

Preface

In this text, we define the Heegner module of an elliptic curve over a global field. For global ground fields of positive characteristic, Drinfeld proved that certain elliptic curves are the images of Drinfeld modular curves. On these modular curves are points corresponding to Heegner points on classical modular curves. These points, called Drinfeld-Heegner points, correspond to generators of the Heegner module of the elliptic curve. Furthermore, for the case of a Weil elliptic curve over the rational field $\mathbb{Q}$, the Heegner module of the curve is generated by the corresponding Heegner points.

The cohomology of the Heegner module of an elliptic curve over a global field induces elements in the cohomology of the elliptic curve. As an application, we prove the Tate conjecture for a class of elliptic surfaces over finite fields. This case of the Tate conjecture is essentially equivalent to the conjecture of Birch and Swinnerton-Dyer for a corresponding class of elliptic curves over global fields and is also equivalent to the finiteness of the Tate-Shafarevich groups of these elliptic curves. This application is parallel to V.A. Kolyvagin's proof of the conjecture of Birch and Swinnerton-Dyer for a class of Weil elliptic curves over the field of rational numbers.

Paris, March 2004 *M.L. Brown*

Contents

1

Introduction

The points of departure of this text are twofold: first the proof by Drinfeld in 1974 ([Dr1], see also Appendix B) of an important case of the Langlands conjecture for GL_2 over a global field of positive characteristic and second the proof by Kolyvagin [K] in 1989 of the Birch Swinnerton-Dyer conjecture for a class of Weil elliptic curves over the rational field $\mathbb{Q}$.

A consequence of Drinfeld's work is that an elliptic curve E over a global field F of positive characteristic with split multiplicative reduction at a place is an image of a Drinfeld modular curve (see Appendix B, §B.11). The analogues of Heegner points on elliptic curves over the rational field $\mathbb{Q}$ may be then constructed on the curve E; these points on E are called Drinfeld-Heegner points.

These Drinfeld-Heegner points satisfy relations given by the action of the Hecke operators on the Drinfeld modular curves. We may then define, by generators and these relations, a *Heegner module* attached to the elliptic curve E. The Drinfeld-Heegner points of E generate a subgroup of E which is a homomorphic image of the Heegner module; nevertheless, the Heegner module is an object distinct from E. The cohomology of the Heegner module may be computed to a large extent (see Chapter 6). As an application of the cohomology of the Heegner module, we may then prove under suitable hypotheses the Tate conjecture for the elliptic surface over a finite field corresponding to the elliptic curve E/F (see Chapter 7).

The final part of the proof of the Tate conjecture (see Chapter 7) is parallel to Kolyvagin's calculation with "Euler systems" (see [R]). In particular, the derived cohomology classes of Kolyvagin transposed to the present case of elliptic curves over function fields arise naturally as part of the cohomology of the Heegner module.

Chapter 7 of this text is the sequel to the paper [Br2], in which we considered the Tate conjecture for surfaces equipped with a rational pencil of elliptic curves; here we consider the general case of surfaces with an irrational elliptic fibration. Furthermore, for the original case of a rational pencil of elliptic curves, we give much more complete results and eliminate some of the technical hypotheses of the main theorem 1.1 of the first paper [Br2].

In this chapter below, we summarise the main results of this text.

1.1 Statement of the Tate conjecture

Let

k be a finite field of characteristic p with $q = p^m$ elements;

$\bar{k}$ be an algebraic closure of k;

C/k be a smooth projective irreducible curve over k;

F be the function field of the curve C;

X/k be an elliptic surface over C; that is to say, X/k is a smooth projective irreducible surface, equipped with a morphism $f : X \to C$ with a section such that all fibres of f, except a finite number, are elliptic curves;

E/F be the generic fibre of $f : X \to C$, which is an elliptic curve E over F;

∞ be a closed point of C.

The zeta function $\zeta(X, s)$ of X is defined by the formula

$$\zeta(X, s) = \prod_{x \in X(\bar{k})} \frac{1}{1 - |\kappa(x)|^{-s}}.$$

By Grothendieck and Deligne, for every prime number $l \neq p$ the zeta function takes the form

$$\zeta(X, s) = \prod_{i=0}^{4} P_i(X, q^{-s})^{(-1)^{i+1}}$$

where we have

(i) $P_i(X,t) = \det(1 - t\Theta |\ H^i_{\text{ét}}(X \times_k \bar{k}, \mathbb{Q}_l))$

$$P_0(X,t) = 1 - t, \quad P_4(X,t) = 1 - q^2 t,$$

where Θ is the Frobenius automorphism of $X \times_k \bar{k}$ relative to k;

(ii) $P_i(X,t) \in \mathbb{Z}[t]$ is independent of the prime number l for all i;

(iii) the roots of $P_i(X,t)$ in $\mathbb{C}$ have absolute values equal to $q^{-i/2}$.

Let $\rho(X)$ be the rank of the Néron-Severi group $\mathrm{NS}(X)$ of X/k. The Tate conjecture for this particular case of a surface over a finite field can be stated in one of these three equivalent ways:

(a) If $l \neq p$, the cycle map

$$\mathrm{NS}(X) \otimes_{\mathbb{Z}} \mathbb{Q}_l \to H^2_{\text{ét}}(X \times_k \bar{k}, \mathbb{Q}_l(1))^{\mathrm{Gal}(\bar{k}/k)}$$

is an isomorphism.

(b) The multiplicity of q as an inverse root of $P_2(X,t)$ is equal to $\rho(X)$.

(c) The order of the pole of $\zeta(X,s)$ at $s=1$ is equal to $\rho(X)$.

[For more details see [Br2, Introduction], [T1], [T3].]

1.2 The Drinfeld modular curve $X_0^{\mathrm{Drin}}(I)$

Let A be the coordinate ring $\Gamma(C \setminus \{\infty\}, \mathcal{O}_c)$ of the affine curve $C \setminus \{\infty\}$. Let I be a non-zero ideal of A.

The curve $X_0^{\mathrm{Drin}}(I)$ is the coarse moduli scheme of Drinfeld modules of rank 2 for A equipped with an I-cyclic subgroup (Definition 2.4.2); this curve is compactified by a finite number of cusps which correspond to "degenerate" Drinfeld modules. The points of $X_0^{\mathrm{Drin}}(I)/F$ correspond to pairs (D,Z) where D is a Drinfeld module of rank 2 for A and Z is a finite closed sub-group scheme of D which is isomorphic to A/I, as an A-module-scheme.

This modular curve $X_0^{\mathrm{Drin}}(I)$ is an analogue for the global field F of the classical modular curve $X_0(N)$ which is the coarse moduli scheme of elliptic curves equipped with a cyclic subgroup of order N, where N is a positive integer.

[For more details see, §2.4.]

1.3 Analogue for F of the Shimura-Taniyama-Weil conjecture

Let E/F be an elliptic curve which admits "split Tate multiplicative reduction" at ∞. Let I be the non-zero ideal of the ring A which is the conductor, without the place at ∞, of the elliptic curve E.

Thanks to the work of Drinfeld on the Langlands conjecture for GL(2), there is a finite surjective morphism of curves

$$\psi : X_0^{\mathrm{Drin}}(I) \to E.$$

This result is the analogue for the global field F of the Shimura-Taniyama-Weil conjecture proved by Wiles [W] for semi-stable elliptic curves over $\mathbb{Q}$.

[For more details, see §4.7 and Appendix B.]

1.4 Drinfeld-Heegner points

Let K be a field which is an quadratic extension of F where the place ∞ remains inert; K is said to be an *imaginary quadratic extension* of F.

Let D be a Drinfeld module for A of rank 2 with complex multiplication by an order $\mathcal{O}$ of K; let Z be an I-cyclic subgroup of D. Then the pair (D, Z) represents a point on the modular curve $X_0^{\text{Drin}}(I)$ (see §1.2).

If the quotient Drinfeld module D/Z has the same ring of endomorphisms $\mathcal{O}$ as D then the point (D, Z) on the modular curve $X_0^{\text{Drin}}(I)$ is called a *Drinfeld-Heegner point* (see chapter 4).

If (D, Z) is a Drinfeld-Heegner point and $\psi : X_0^{\text{Drin}}(I) \to E$ is a finite surjective morphism of curves, where E is an elliptic curve over F (see §1.3), then the point $\psi(D, Z)$ is called a *Drinfeld-Heegner point* of the elliptic curve E.

The Drinfeld-Heegner points (D, Z) and $\psi(D, Z)$ are rational over the ring class field $K[c]$, where c is the conductor of the order $\mathcal{O}$ of K relative to A (see §§2.2,2.3).

1.5 Heegner sheaves

Let E/F be an elliptic curve equipped with a finite surjective morphism of curves

$$\psi : X_0^{\text{Drin}}(I) \to E.$$

where I is the conductor, without the place at ∞, of E (see §1.3).

Let F^{sep} be a separable closure of the field F. The set of Drinfeld-Heegner points of E generates a subgroup $\mathcal{H}$ of the abelian group $E(F^{\text{sep}})$ of F^{sep}-rational points of E. The group $\mathcal{H}$ equipped with its action by the Galois group $\text{Gal}(F^{\text{sep}}/F)$ is then a sheaf of abelian groups for the étale topology of Spec F (see chapter 4) where for any étale morphism $U \to \text{Spec } F$ we have

$$\Gamma(U, \mathcal{H}) = \left\{ f : U \to E \;\middle|\; \begin{array}{c} \text{the geometric points of} \\ \text{the image of } f \text{ are Drinfeld} - \text{Heegner} \end{array} \right\}.$$

Evidently $\mathcal{H}$ is a subsheaf of the étale sheaf defined by the elliptic curve E.

In the same way, the set of Drinfeld-Heegner points of $X_0^{\text{Drin}}(I)$ defines a sheaf of sets for the étale topology on Spec F. Furthermore, a sheaf of abelian groups may be defined for the étale topology on the curve C and which is the subsheaf generated by the Drinfeld-Heegner points of the sheaf defined by the Néron model of E over C .

1.6 Hecke operators

Let z be a closed point of $C \setminus \{\infty\}$ let $\mathfrak{m}_z$ be the maximal ideal of the ring A defined by z. If z is not in the support of Spec A/I, the Hecke operator T_z is defined on the curve $X_0^{\mathrm{Drin}}(I)$ by

$$T_z : (D, Z) \mapsto \sum_H (D/H, (Z+H)/H)$$

where H runs over the $\mathfrak{m}_z$-cyclic subgroups of D and the right hand side of this formula is a divisor on $X_0^{\mathrm{Drin}}(I)$.

[See §4.5 for more details.]

1.7 Bruhat-Tits buildings with complex multiplication

Let $\Delta(\mathrm{SL}_2(F))$ be the euclidean Bruhat-Tits building for SL_2 of the field F equipped with its discrete valuation associated to a closed point z. For this case of SL_2, the building $\Delta(\mathrm{SL}_2(F))$ is a *tree*.

Let $\mathcal{L}$ be the set of vertices of $\Delta(\mathrm{SL}_2(F))$. Then a *Bruhat-Tits tree with complex multiplication* is a couple $(\Delta(\mathrm{SL}_2(F)), \mathrm{Exp})$ where Exp, called an *exponent function*, is a map of sets (see chapter 3)

$$\mathrm{Exp} : \mathcal{L} \to \mathbb{Z}.$$

We are principally concerned with Bruhat-Tits buildings with complex multiplication which arise in the following way. Let

M be a reduced 2-dimensional commutative F-algebra;
R be the discrete valuation ring of F associated to the closed point z;
π be a uniformising parameter of R;
S be the integral closure of R in M.

As M is a 2-dimensional vector space over F, the R-lattices contained in M correspond surjectively to the elements of $\mathcal{L}$. Two R-lattices Λ_1, Λ_2 in M correspond to the same point in $\mathcal{L}$ if and only if they are equivalent, that is, $\Lambda_1 = a\Lambda_2$ for some $a \in F^*$.

To each lattice equivalence class $[\Lambda] \in \mathcal{L}$, where $\Lambda \subset M$ is a lattice of M, is associated the ring of endomorphisms $\mathrm{End}_R^M(\Lambda)$ which is the subring of M preserving Λ:

$$\mathrm{End}_R^M(\Lambda) = \{m \in M \mid m\Lambda \subset \Lambda\}.$$

The ring $\mathrm{End}_R^M(\Lambda)$ is uniquely determined by its conductor ideal $[S : \mathrm{End}_R^M(\Lambda)]$, which is an ideal of R, and depends only on the lattice class of Λ. The conductor $[S : \mathrm{End}_R^M(\Lambda)]$ is of the form $\pi^{\mathrm{Exp}([\Lambda])}R$, where the exponent of the conductor $\mathrm{Exp}([\Lambda])$ is an integer; this defines a map

$$\mathrm{Exp} : \mathcal{L} \to \mathbb{Z}.$$

This pair $(\Delta(\mathrm{SL}_2(F)), \mathrm{Exp})$ is a Bruhat-Tits building with complex multiplication. When the algebra M is not reduced, a Bruhat-Tits building with complex multiplication may also be defined (chapter 3).

This construction may be globalised to define a *Bruhat-Tits net with complex multiplication* for any excellent Dedekind domain R (see §§3.9, 3.10, 3.11).

1.8 Bruhat-Tits buildings with complex multiplication and Drinfeld-Heegner points

Let (D, Z) be a Drinfeld-Heegner point on $X_0^{\mathrm{Drin}}(I)$ relative to the imaginary quadratic field extension K of F (see §1.4). Let z be a closed point of $C \setminus \{\infty\}$ where z is not in the support of Spec A/I; let T_z be the Hecke operator at z. Then

$$T_z(D, Z)$$

is a divisor on $X_0^{\mathrm{Drin}}(I)$ whose irreducible components are also Drinfeld-Heegner points.

The Drinfeld module D, which has complex multiplication by an order of K, corresponds to an A-sublattice Λ of rank 2 of K, under the equivalence between Drinfeld modules of infinite characteristic and lattices. Hence D corresponds via Λ to a vertex v of the Bruhat-Tits building $\Delta(\mathrm{SL}_2(F))$ with respect to the discrete valuation on F corresponding to z. The irreducible components of $T_z(D, Z)$ then correspond to the neighbouring vertices of v in $\Delta(\mathrm{SL}_2(F))$. The exponents at z of the conductors of the endomorphism rings of these components of $T_z(D, Z)$ are then the values of an exponent function Exp on the corresponding vertices of $\Delta(\mathrm{SL}_2(F))$.

The endomorphism rings of the components of $T_z(D, Z)$ are in this way described by a Bruhat-Tits tree with complex multiplication $(\Delta(\mathrm{SL}_2(F)), \mathrm{Exp})$ with respect to z (see §§3.6-3.8).

1.9 Classification of Bruhat-Tits buildings with complex multiplication

Let M, R, z be as in §1.7. Let $(\Delta(\mathrm{SL}_2(F)), \mathrm{Exp})$ be the corresponding Bruhat-Tits tree with complex multiplication.

We prove that there are precisely 4 distinct forms of the Bruhat-Tits trees with complex multiplication $(\Delta(\mathrm{SL}_2(F)), \mathrm{Exp})$, that is to say, 4 distinct forms of the exponent functions Exp; there are 3 forms corresponding to the splitting of the place z in the quadratic extension of algebras M/F and there is a 4th form when M is not a reduced algebra.

We give a simple formula for the exponent functions Exp in terms of the standard metric on the euclidean building $\Delta(\mathrm{SL}_2(F))$ (see theorems 3.7.3, 3.7.5 and figures 1, 2, 3, and 4 of §3.8).

1.10 The Heegner module of a galois representation

Let

ρ be a finite dimensional continuous representation over a local field L of the galois group $\mathrm{Gal}(F^{\mathrm{sep}}/F)$, where F^{sep} denotes the separable closure of F;
K/F be an imaginary quadratic field extension;
R be a subring of L such that the character of ρ takes its values in R.

We construct a discrete galois R-module $\mathcal{H}(\rho)$ over $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ called the *canonical Heegner module attached to ρ and K/F with coefficients in R.*

The Heegner module $\mathcal{H}(\rho)$ is defined by generators and relations over the ring R. The generators are the symbols $< b, c >$ where c runs over all effective divisors on Spec A and b runs over all divisor classes of $\mathrm{Pic}(O_c)$, the Picard group of the order O_c of K with conductor c. The relations are explicitly given in (5.3.5)-(5.3.8); they are derived from the action of the Hecke operators on Drinfeld-Heegner points.

The most important case of this construction of $\mathcal{H}(\rho)$ arises from elliptic curves. Suppose that E/F is an elliptic curve equipped with a finite surjective morphism of curves

$$\psi : X_0^{\mathrm{Drin}}(I) \to E.$$

For any prime number l different from the characteristic of F, the curve E provides a continuous l-adic representation

$$\sigma : \mathrm{Gal}(F^{\mathrm{sep}}/F) \to \mathrm{End}_{\mathbb{Q}_l}(H^1_{\mathrm{\acute{e}t}}(E \times_F F^{\mathrm{sep}}, \mathbb{Q}_l)).$$

Let K/F be an imaginary quadratic extension field of F in which all primes dividing the conductor of E, except ∞, split completely. The character of this representation σ takes its values in $\mathbb{Z}$. The Heegner module $\mathcal{H}(\sigma)$ attached to σ and K/F is then an abelian group equipped with the structure of a discrete $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-module; it is also equipped with a galois-equivariant homomorphism (see examples 5.3.18)

$$f : \mathcal{H}(\sigma)^{(0)} \to E(F^{\mathrm{sep}})$$

where $\mathcal{H}(\sigma)^{(0)}$ is the direct summand of $\mathcal{H}(\sigma)$ generated by the symbols $< b, c >$ where c runs over all effective divisors on Spec A prime to a particular finite exceptional set of prime divisors. The image of this homomorphism is precisely the subgroup of $E(F^{\mathrm{sep}})$ generated by the Drinfeld-Heegner points; that is to say, the image $f(\mathcal{H}(\sigma)^{(0)})$ may be considered as a sheaf of abelian groups for the étale topology on Spec K and it coincides with the Heegner sheaf $\mathcal{H}$ of E, as in §1.5.

[See chapter 5 for more details.]

1.11 Cohomology of the Heegner module

As in the preceding section §1.10, let $\mathcal{H}(\rho)$ over $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ be the Heegner module over R attached to ρ, K/F, and R.

The Heegner module $\mathcal{H}(\rho)$ is an *abelian representation* of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ in that the action of this galois group factors through an abelian quotient.

More precisely, let $K[c]$ be the ring class field of K over F with conductor c (§2.3). Then $\mathcal{H}(\rho)$ may be expressed as a direct limit

$$\mathcal{H}(\rho) = \varinjlim \mathcal{H}_c$$

where c runs over all effective divisors on Spec A and $\mathcal{H}_c$ is a $\mathrm{Gal}(K[c]/K)$-module and is an R-module of finite type. This direct limit (which under a simple hypothesis is a direct union; see corollary 5.9.4) defines a filtration on $\mathcal{H}(\rho)$ and gives this Heegner module the structure of a discrete module over the abelian galois group

$$\mathrm{Gal}(\bigcup_c K[c]/K).$$

For any R-algebra S and any prime divisor z in the support of c, we attempt to determine in Chapter 6 the galois cohomology groups

$$H^i(\mathrm{Gal}(K[c]/K[c-z]), \mathcal{H}_c \otimes_R S), \quad \text{for } i \geq 0.$$

This is the first step in the determination of the galois cohomology groups

$$H^i(\mathrm{Gal}(K^{\mathrm{sep}}/K), \mathcal{H}(\rho) \otimes_R S), \quad \text{for } i \geq 0.$$

The most precise results we obtain are for the case where S is an *infinitesimal trait* that is to say an artin local ring which is a quotient of a discrete valuation ring.

[See chapter 6 for more details.]

1.12 The Tate conjecture and the Heegner module

Let $\mathcal{E}/C$ be the Néron model of the elliptic curve E/F. Then $\mathcal{E}$ can be considered as a sheaf of abelian groups on C for the étale topology.

The *Tate-Shafarevich group of* E/F is defined by

$$\text{Ш}(E,F) = H^1_{\text{ét}}(C,\mathcal{E}).$$

As k is a perfect field, this says that Ш(E,F) is the group of principal homogeneous of E/F which are everywhere locally trivial. Thanks to the work of Artin, Tate and Milne, the finiteness of the group Ш(E,F) is equivalent to the Tate conjecture for the elliptic surface $\mathcal{E}/k$ of §1.1.

Suppose that E/F is an elliptic curve equipped with a finite surjective morphism of curves over F

$$\psi : X_0^{\mathrm{Drin}}(I) \to E.$$

For any prime number l different from the characteristic of F, we have a continuous l-adic representation

$$\rho : \mathrm{Gal}(F^{\mathrm{sep}}/F) \to \mathrm{End}_{\mathbb{Q}_l}(H^1_{\text{ét}}(E \times_F F^{\mathrm{sep}}, \mathbb{Q}_l)).$$

Let K/F be an imaginary quadratic extension field of F in which all primes dividing the conductor of E, except ∞, split completely. As in §1.10, let $\mathcal{H}(\rho) = \varinjlim \mathcal{H}_c$ be the Heegner module attached to ρ and K/F and the ring of coefficients $\mathbb{Z}$; we have a morphism of sheaves for the étale topology over Spec K

$$f : \mathcal{H}(\rho)^{(0)} \to E.$$

The morphism of sheaves f provides homomorphisms of cohomology groups

$$\left(\mathcal{H}_c \otimes_{\mathbb{Z}} \frac{\mathbb{Z}}{n\mathbb{Z}}\right)^{\mathrm{Gal}(K[c]/K)} \to H^1_{\text{ét}}(\mathrm{Spec}\ K[c], E_n)^{\mathrm{Gal}(K[c]/K)}$$

for all integers $n \geq 1$ prime to the characteristic of F and all c prime to a finite exceptional set of divisors, where E_n is the n-torsion subgroup of E. This gives rise (see (7.14.5)) to the fundamental *Heegner homomorphism*, for all n prime to a finite exceptional set of prime numbers,

$$\left(\mathcal{H}_c \otimes_{\mathbb{Z}} \frac{\mathbb{Z}}{n\mathbb{Z}}\right)^{\mathrm{Gal}(K[c]/K)} \to H^1_{\text{ét}}(\mathrm{Spec}\ K, E).$$

The subgroups of $H^1_{\text{ét}}(\mathrm{Spec}\ K, E)$ coming from the calculation of the cohomology of the Heegner module $\mathcal{H}(\rho)$, by a fine analysis in Chapter 7, enables us to show, under suitable hypotheses, the finiteness of the Tate-Shafarevich group Ш(E, F) and hence to prove the Tate conjecture for $\mathcal{E}/k$.

1.13 Statement of the main result on the Tate conjecture

In this section, let F be a global field of positive characteristic and with exact field of constants k; fix a place ∞ of F with residue field equal to k. Let E/F be an elliptic curve with an origin and with split multiplicative reduction at ∞. Then E/F is equipped with a map of F-schemes

$$\pi : X_0^{\mathrm{Drin}}(I) \to F$$

where I, which is an ideal of A, is the conductor of E without the component at ∞ (see §1.3). Let K be an imaginary quadratic extension field of F for