Remarks on the elliptic cohomology of finite groups

By

Michimasa TANABE

1. Elliptic character

Let *Ell**(?) be the elliptic cohomology based on the Weierstrass cubic

 $y^2 = 4x^3 - g_2x - g_3$

over

$$Ell^* = \mathbb{Z}[1/6][g_2, g_3, \Delta^{-1}](\Delta = g_2^3 - 27g_3^2)$$

(see [3], [11]). The coefficient ring $Ell^* = Ell^*(\text{pt})$ can be viewed as the ring of modular forms on $\Gamma(1) = SL_2(\mathbb{Z})$ over $\mathbb{Z}[1/6]$. (The grading on Ell^* is given by $-2 \times \text{weight.}$) In other words Ell^* is the ring which represents the functor

 $\{\mathbf{Z}[1/6]\)$ -algebras $A\} \rightarrow \{\text{isomorphism classes of } \Gamma(1)\)$ -test objects over $A\}$

with universal test object

 $(E_{\text{univ}}, \omega_{\text{univ}}) = (y^2 = 4x^3 - g_2x - g_3, dx/y),$

where a $\Gamma(1)$ -test object over A means a pair (E, ω) consisisting of an elliptic curve E/A and a nowhere-vanishing invariant differential ω on E (see [10, Chapter II]). This identification is *natural* in the sense that the formal group law associated to Ell with canonical orientation is the formal group \hat{E}_{univ} associated to E_{univ} , with parameter T = -2x/y.

For $n \ge 2$ let $E_{2n} \in Ell^{-4n} \otimes \mathbf{Q}$ be the Eisenstein series given by the *q*-expansion

$$E_{2n}(q) = 1 - (4n/B_{2n}) \sum_{k\geq 1} \sigma_{2n-1}(k)q^k$$

where

$$z/(e^{z}-1)=1-z/2+\sum_{n\geq 1}B_{2n}z^{2n}/(2n)!$$

Received October 1, 1993

and

$$\sigma_n(k) = \sum_{d|k} d^n.$$

Then the Tate elliptic curve Tate(q) is given over $\mathbf{Z}[1/6]((q))$ by

$$y^2 = 4x^3 - \frac{1}{12}E_4(q)x + \frac{1}{216}E_6(q)$$

and there is a unique ring homomorphism

 $\lambda: Ell^* \rightarrow \mathbb{Z}[1/6]((q))$

classifying (Tate(q), dx/y). (This λ is nothing but a q-expansion homomorphism which is injective.) Since the formal group associated to Tate(q), viewed as G_m/q^z , is canonically isomorphic to formal multiplicative group \hat{G}_m we have a canonical isomorphism of formal groups over $\mathbb{Z}[1/6]((q))$:

 $\theta: \widehat{\mathbf{G}}_m \xrightarrow{\cong} \lambda_* \widehat{E}_{\text{univ.}}$

This isomorphism θ is actually a strict isomorphism of formal group laws, where we take local parameter T = t - 1 for $G_m = \text{Spec } \mathbb{Z}[t, t^{-1}]$. Therefore, by using the theory of Landweber-Novikov operations, we have

Theorem 1.1 ([13]). There is a unique natural transformation of multiplicative cohomology theories on finite CW-complexes

 $\lambda(X): Ell^*(X) \rightarrow K^*(X)[1/6]((q))$

such that :

(1) $\lambda(pt) = \lambda$.

(2) Let $\lambda(CP^{\infty}) = \lim_{n \to \infty} \lambda(CP^{n})$ and denote by x^{Ell} (resp. x^{K}) the canonical orientation for Ell (resp. K) then

 $\lambda(CP^{\infty})(x^{Ell}) = \theta(x^{K}).$

Here $K^*(?)$ is $\mathbb{Z}/(2)$ -graded complex K-theory.

The above λ (?) is called elliptic character.

2. Modularity of elliptic character for finite groups

Let *G* be a finite group and *BG* be its classifying space. Since $\lim^{1} K^{*}(BG_{i})=0$ for a filtration $\{BG_{i}\}$ on *BG* consisting of finite subcomplexes we have elliptic character

 $\lambda(BG): Ell^*(BG) \rightarrow K^*(BG)[1/6]((q)).$

Using Atiyah's isomorphism $K^*(BG) \cong \hat{R}(G)$ ([1]), we have a natural ring homomorphism

 $Ell^*(BG) \rightarrow \widehat{R}(G)[1/6]((q)),$

where $\hat{R}(G)$ denotes the completion of the complex representation ring of G at the ideal consisting of the virtual representations of dimension 0.

For a prime p let $G_{1,p} = \{g \in G : g^{p^N} = 1, N \gg 0\}$, $R_p(G) = (\hat{R}(G))_p^{\circ}$ and denote by C_p the completion of the algebraic closure of \mathbf{Q}_p . Then there is a character map

$$\chi_p(G): R_p(G) \to \operatorname{Map}_G(G_{1,p}, \mathbb{C}_p)$$

which is a *p*-adic analogue of the usual group character (see [6]). Thus for a prime $p \ge 5$ (from now on we fix a prime $p \ge 5$) we have a natural ring homomorphism

$$\lambda_p(G): Ell^*(BG) \rightarrow \operatorname{Map}_G(G_{1,p}, \mathbf{C}_p((q))).$$

We shall study modularity property of this $\lambda_{p}(G)$. Before stating our result we give a brief account of *p*-adic theory of modular forms.

Let $V(n) = V(\mathbf{Z}_p[\zeta_{p^n}], \Gamma(1))$ be the ring of $\Gamma(1)$ -generalized *p*-adic modular functions over $B_n = \mathbf{Z}_p[\zeta_{p^n}]$, where ζ_{p^n} is a primitive p^n -th root of unity (see [10, Chapter V], [5, Chapter I]). The ring V(n) represents the functor

 $\{p\text{-adic } B_n\text{-algebras } A\} \rightarrow \{\text{isomorphism classes of trivialized elliptic curves over } A\}.$

Here a *p*-adic B_n -algebra means a B_n -algebra which is complete Hausdorff in its *p*-adic topology and a trivialized elliptic curve over A means a pair (E, φ) consisting of an elliptic curve E/A and a trivialization φ of it, i.e., an isomorphism of formal groups over A:

 $\varphi: \widehat{E} \xrightarrow{\cong} \widehat{\mathbf{G}}_m.$

There is an obvious inclusion

$$V(n) \hookrightarrow V(n+1)$$

for every $n \ge 0$.

The Tate curve Tate(q), viewed over $\widehat{B_n((q))} = (B_n((q)))_p^{\wedge}$, has a canonical trivialization

$$\varphi_{\operatorname{can}} = \theta^{-1} : \operatorname{Tate}(q) \xrightarrow{\cong} \widehat{\mathbf{G}}_m.$$

Then evaluation on $(Tate(q), \varphi_{can})$ gives an injective q-expansion homomorphism

$$\widetilde{\lambda}$$
: $V(n) \rightarrow \widehat{B}_n((q))$.

For any $a \in \mathbb{Z}_{P}^{\times}$ and $f \in V(n)$ we define $[a] f \in V(n)$ by the formula

$$[a]f(E, \varphi)=f(E, a^{-1}\varphi),$$

where a^{-1} acts on φ via an automorphism of $\hat{\mathbf{G}}_m$. This gives the action of \mathbf{Z}_p^{\times} on V(n). Let

$$V^{k}(n) = \{f \in V(n) : [a]f = a^{k}f(\forall a \in \Gamma_{n})\}$$

and

$$V^*(n) = \bigoplus_{k} V^k(n),$$

where $\Gamma_n = \{a \in \mathbb{Z}_p^{\times} : a \equiv 1(p^n)\}$. Note that there is an obvious inclusion

$$V^{k}(n) \hookrightarrow V^{k}(n+1)$$

since $\Gamma_{n+1} \subset \Gamma_n$.

Let dT/(1+T) be the standard invariant differential on $\hat{\mathbf{G}}_m$. Then for any trivialized elliptic curve (E, φ) we have an invariant differential $\varphi^*(dT/(1+T))$ on \hat{E} which uniquely extends to a nowhere vanishing invariant differential on E. Thus for any $f \in Ell^{2k}$ we get an element $\tilde{f} \in V^{-k} = V^{-k}(0)$ defined by

$$\widetilde{f}(E, \varphi) = f(E, \varphi^*(dT/(1+T))).$$

Therefore there is a ring homomorphism

 $Ell^* \rightarrow V$

which preserves q-expansions and hence is injective. When we regard Ell^* as a subring of V via this homomorphism $E_{univ} \otimes V$ admits a trivialization φ_{univ} given by

$$\varphi_{\text{univ}}(T) = \exp_{\mathbf{G}_{\pi}}(\log_{\hat{E}_{\text{univ}}}(T)) \in V[[T]].$$

For $(E_{univ} \otimes V, dx/y)$ is clearly isomorphic to $(E, \varphi^*(dT/(1+T)))$ as $\Gamma(1)$ -test objects for any universal trivialized elliptic curve (E, φ) over V and

 $dx/y = d \log_{\hat{E}_{univ}} (T)(T = -2x/y)$

and

$$\varphi^*(dT/(1+T)) = d \log_{G_*}(\varphi(T)).$$

Theorem 2.1. For any $x \in Ell^{2k}(BG)$ and $g \in G$ of order p^n there is a (necessarily unique) element $f \in V^{-k}(n)$ such that

$$[\lambda_{P}(G)(x)](g) = f(\text{Tate}(q), \varphi_{can}).$$

Proof. First consider the case $G = \mathbb{Z}/p^n\mathbb{Z}$ and $g = g_n$ (the canonical generator of $\mathbb{Z}/p^n\mathbb{Z}$).

Let

$$f_n = \varphi_{\text{univ}}^{-1}(\zeta_{p^n} - 1) \in pV(n).$$

Then f_n has weight -1 over Γ_n , i.e.,

$$f_n \in pV(n) \cap V^{-1}(n) = pV^{-1}(n)$$

since, for any $a \in \Gamma_n$,

$$[a]f_{n} = [a](\varphi_{\text{univ}}^{-1}(\zeta_{p^{n}} - 1))$$

= [a]((exp_{\bar{E}_{unv}} \log_{\bar{G}_{*}})(\zeta_{p^{n}} - 1))
= (exp_{[a]_{*}\bar{E}_{unv}} \log_{\bar{G}_{*}})(\zeta_{p^{n}} - 1)
= ((a⁻¹ exp_{\bar{E}_{unv}} a) log_{\bar{G}_{*}})(\zeta_{p^{n}} - 1)
= a^{-1}(exp_{\bar{E}_{unv}} \log_{\bar{G}_{*}})(\zeta_{p^{n}}^{a} - 1)
= a⁻¹f_n.

Now the q-expansion of f_n is given by

$$f_n(\text{Take}(q), \varphi_{\text{can}}) = \tilde{\lambda}(f_n)$$

= $\tilde{\lambda}((\exp_{\hat{E}_{\text{univ}}} \log_{\hat{G}_n})(\zeta_{p^n} - 1))$
= $(\exp_{\lambda_* \hat{E}_{\text{univ}}} \log_{\hat{G}_n})(\zeta_{p^n} - 1)$
= $\theta(\zeta_{p^n} - 1).$

Therefore for any $x = \sum_{i} a_i (x^{Eil})^i$ of degree 2k in

$$Ell^{*}(B\mathbf{Z}/p^{n}\mathbf{Z}) = Ell^{*}[[x^{Ell}]]/([p^{n}]_{\bar{E}_{unv}}(x^{Ell})),$$
$$[\lambda_{p}(\mathbf{Z}/p^{n}\mathbf{Z})(x)](g_{n}) = \sum_{i} \lambda(a_{i})[\theta(\chi_{p}(\mathbf{Z}/p^{n}\mathbf{Z})(x^{K}))^{i}](g_{n})$$
$$= \sum_{i} \lambda(a_{i})\theta(\zeta_{p^{n}}-1)^{i}$$
$$= (Take(q), \varphi_{can})$$

for $f = \sum_{i} a_{i} f_{n}^{i} \in V^{-k}(n)$. This proves the result for $G = \mathbb{Z}/p^{n}\mathbb{Z}$ and $g = g_{n}$.

Now for a general G and $g \in G$ of order p^n there is a unique homomorphism

$$\alpha: \mathbf{Z}/p^{n}\mathbf{Z} \rightarrow G$$

which sends g_n to g. Hence for any $x \in Ell^{2k}(BG)$

M. Tanabe

$$egin{aligned} & [\lambda_{p}(G)(x)](g) = [\lambda_{p}(G)(x)]lpha(g_{n})) \ & = [\lambda_{p}(\mathbf{Z}/p^{n}\mathbf{Z})(lpha^{*}x)](g_{n}) \ & = f(\mathrm{Tate}(q), \ arphi_{\mathrm{can}}) \end{aligned}$$

for some $f \in V^{-k}(n)$.

Remark 2.2. The above result asserts that every element in Im $\lambda_p(G)$ is *p*-adically Thompson series.

3. Relations between elliptic character and HKR character

Throughout this section we denote simply by Ell the *p*-adic completion of Ell. (Recal that *p* is a fixed prime ≥ 5 .)

Let \mathcal{O}_{P} be the valuation ring of C_{P} and \mathfrak{p}_{P} be the valuation ideal. Let m be a maximal homogeneous ideal of Ell^{*} (= $\mathbb{Z}_{P}[g_{2}, g_{3}, \mathcal{A}^{-1}]$) containing (p, E_{P-1}) and choose a local homomorphism

 $\psi: (Ell^*)_m^{\wedge} \to \mathcal{O}_p.$

The restriction of ψ on Ell^* classifies an elliptic curve over \mathcal{O}_P whose mod \mathfrak{p}_P reduction is supersingular (see [18, Chapter V §§3-4] and [9, §§2.0-1]).

Theorem 3.1[7], [8], [6]. Let $G_{2,p} = \{(g, h) \in G^2 : [g, h] = 1, g^{pN} = h^{pN} = 1, N \gg 0\}$. Then there is a generalized character map

$$(Ell_{\mathfrak{m}}^{\wedge})^*(BG) \rightarrow \operatorname{Map}_G(G_{2,p}, \mathbb{C}_p)$$

which extends to the isomorphism

 $(Ell^{\wedge}_{\mathfrak{m}})^*(BG)\otimes_{(Ell^{\wedge})^*} \mathbb{C}_p \xrightarrow{\cong} \operatorname{Map}_G(G_{2,p}, \mathbb{C}_p).$

To relate the above character map to elliptic character we need to specify an exponential isomorphism

 $(\mathbf{Q}_p/\mathbf{Z}_p)^2 \xrightarrow{\cong} \widehat{E}_{\mathrm{univ}}(\mathfrak{p}_p)_{\mathrm{tors}}$

as described in [6]. This requires some facts about elliptic curves and modular forms.

Let $M^*(n) = M^*(B_n, \Gamma(p^n)^{\operatorname{arith}})$ (resp. $M_1^*(n) = M^*(B_n, \Gamma_1(p^n)^{\operatorname{arith}})$) be the ring of $\Gamma(p^n)^{\operatorname{arith}}$ (resp. $\Gamma_1(p^n)^{\operatorname{arith}}$)-modular forms over $B_n = \mathbb{Z}_p[\zeta_{p^n}]$ (see [10, Chapter II]). These rings represent the functors

 $\{B_n\text{-algebras }A\} \rightarrow \{\text{isomorphism classes of } \Gamma(p^n)^{\text{arith}}\text{-test objects over }A\}$

and

 $\{B_n\text{-algebras } A\} \rightarrow \{\text{isomorphism classes of } \Gamma_1(p^n)^{\text{arith}}\text{-test objects over } A\}$

respectively. Here a $\Gamma(p^n)^{\operatorname{arith}}$ (resp. $\Gamma_1(p^n)^{\operatorname{arith}}$)-test object over A means a triple (E, ω, β) (resp. (E, ω, ι)) consisting of an elliptic curve E/A, a nowhere vanishing invariant differential ω on E, and a $\Gamma(p^n)^{\operatorname{arith}}$ (resp. $\Gamma_1(p^n)^{\operatorname{arith}}$)-structure β (resp. ι) on E which is an isomorphism (resp. inclusion) of A-group schemes :

$$\beta: \mu_{p^n} \times \mathbf{Z}/p^n \mathbf{Z} \xrightarrow{=} E[p^n]$$

and

$$\iota: \mu_{p^n} \hookrightarrow E[p^n],$$

where $E[p^n]$ denotes the kernel of multiplication by p^n on E.

For every $n \ge 0$ there are natural inclusions, which do *not* preserve *q*-expansions,

$$M^*(n) \hookrightarrow M^*(n+1)$$

and

$$M_1^*(n) \hookrightarrow M^*(n)$$

since a $\Gamma(p^n)^{\text{arith}}$ -structure β gives a $\Gamma(p^{n-1})^{\text{arith}}$ -structure $\beta|\mu_{p^{n-1}} \times p\mathbf{Z}/p^n\mathbf{Z}$ and a $\Gamma_1(p^n)^{\text{arith}}$ -structure $\beta|\mu_{p^n}$. The first inclusion has the effect $q \mapsto q^p$ on the *q*-expansions and the second one has the effect $q \mapsto q^{p^n}$. There is also a *q*-expansion preserving natural inclusion

$$M_1^*(n) \hookrightarrow M_1^*(n+1)$$

which is compatible with the above ones.

Any trivialized elliptic curve (E, φ) over A has a $\Gamma_1(p^n)^{\operatorname{arith}}$ -structure given by the trivialization

 $\varphi^{-1}|\mu_{p^n}: \mu_{p^n} \hookrightarrow E[p^n].$

Therefore we have a $\Gamma_1(p^n)^{\text{arith}}$ -test object $(E, \varphi^*(dT/(1+T)), \varphi^{-1}|\mu_{p^n})$ over A and a *q*-expansion preserving ring homomorphism

 $M_1^*(n) \rightarrow V^*(n)$

which is necessarily injective.

Let

$$\beta(n)_{\text{univ}}: \ \mu_{p^n} \times \mathbb{Z}/p^n \mathbb{Z} \xrightarrow{=} (E_{\text{univ}} \otimes M^*(n))[p^n]$$

be a universal $\Gamma(p^n)^{\text{arith}}$ -structure. Let $Ell^*(n)$ be the integral closure of Ell^* in $M^*(n) (M^*(n)[1/p]$ is itself integral over $Ell^*[1/p]$), \mathfrak{m}_n be a maximal ideal of $Ell^*(n)$ containing $\mathfrak{m}Ell^*(n)$, and $\mathfrak{m}_n = \mathfrak{m}_n(Ell^*(n))_{\mathfrak{m}_n}$. Then the isomorphism

$$(\mathbf{Z}/p^{n}\mathbf{Z})^{2} \xrightarrow{\cong} E_{\text{univ}}[p^{n}](M^{*}(n))$$

given by

 $(a, b) \mapsto \beta(n)_{\text{univ}}(\zeta_{p^n}^a, b)$

induces an isomorphism

$$\widehat{\beta(n)}_{\text{univ}}: (\mathbf{Z}/p^n\mathbf{Z})^2 \xrightarrow{\cong} \widehat{E}_{\text{univ}}[p^n](\widehat{\mathfrak{m}}_n)$$

since $E_{univ} \otimes Ell^*/m$ is supersingular (cf. [18, Theorem V.3.1 and Proposition VII.2.2]). Here we may assume that

$$\widehat{\beta}(n)_{\text{univ}}(a, 0) = \varphi_{\text{univ}}^{-1}(\zeta_{p^n}^a - 1)(\forall a \in \mathbb{Z}/p^n\mathbb{Z}).$$

Therefore we have an exponential isomorphism given by

$$(a, b) \mapsto \widetilde{\psi}(\widehat{\beta(n)}_{univ}(p^n a, p^n b)) \Big(\forall (a, b) \in \Big(\frac{1}{p^n} \mathbb{Z}/\mathbb{Z}\Big)^2 \Big)$$

and the generalized character map factors as

 $(Ell^{\wedge}_{\mathfrak{m}})^{*}(BG) \rightarrow \operatorname{Map}_{G}(G_{2,p}, \widetilde{Ell^{*}(\infty)}) \rightarrow \operatorname{Map}_{G}(G_{2,p}, \mathbb{C}_{p}),$

where $\widehat{Ell^*(\infty)} = \bigcup_n Ell^*(n)_{\mathfrak{m}_n}^{\wedge}$ and

$$\widetilde{\psi}: \widetilde{Ell}^*(\infty) \to \mathcal{O}_p$$

is an extension of ψ . (We assume that $\mathfrak{m}_n \supset \mathfrak{m}_{n-1} Ell^*(n) (\forall n \ge 1)$.) Let

$$\chi_{2,p}(G): Ell^*(BG) \to \operatorname{Map}_G(G_{2,p}, \widetilde{Ell}(\infty))$$

denote the composition

$$Ell^*(BG) \rightarrow (Ell^{\wedge})^*(BG) \rightarrow \operatorname{Map}_{G}(G_{2,p}, \widetilde{Ell^*(\infty)}).$$

Theorem 3.2. For any $x \in Ell^*(BG)$ and $g \in G$ of order p^n , $\chi_{2,p}(x)(g, 1)$ lies in $(Ell^*(n) \cap M_1^*(n))_p^{\wedge} \hookrightarrow V(n))$ and

$$\lambda_p(x)(g) = [\chi_{2,p}(x)(g, 1)](\operatorname{Tate}(q), \varphi_{\operatorname{can}}).$$

Proof. By using naturality, as in the proof of 2.1, it is enough to show the result for $G = \mathbf{Z}/p^n \mathbf{Z}$ and $g = g_n$. By the construction of HKR character and our choice of an exponential isomorphism, for any $x = \sum_i a_i (x^{\mathcal{E}ll})^i \in Ell^* (B\mathbf{Z}/p^n \mathbf{Z})$,

$$\chi_{2,p}(x)(g_n, 1) = \sum_i a_i \widehat{\beta}(n)_{\text{univ}}(1, 0)^i$$
$$= \sum_i a_i \varphi_{\text{univ}}^{-1}(\zeta_{p^n} - 1)^i$$

 $=\sum_{i} a_{i} f_{n}^{i}$

Therefore we have

 $\lambda_{p}(x)(g_{n}) = \chi_{2,p}(x)(g_{n}, 1)(\operatorname{Tate}(q), \varphi_{\operatorname{can}}).$

Remark 3.3. The above relations between λ_{P} and $\chi_{2,P}$ are analogous to relations between moonshine and generalized moonshine.

DEPARTMENT OF MATHEMATICS KYOTO UNIVERSITY

References

- [1] M. F. Atiyah, Characters and cohomology of finite groups, Publ. Math. IHES, 9 (1961), 23-64.
- [2] A. Baker, On the homotopy type of the spectrum representing elliptic cohomology, Proc. AMS, 107 (1989), 537-548.
- [3] A. Baker, Hecke operators as operations in elliptic cohomology, J. Pure Appl. Alg., 63 (1990), 1-11.
- [4] J-L. Brylinski, Representations of loop groups, Dirac operators on loop space, and modular forms, Topology, 29 (1990), 461-480.
- [5] F. Q. Gouvea, Arithmetic of p-adic Modular Forms, Lect. Notes in Math. 1304, Springer, 1988.
- [6] M. J. Hopkins, Characters and elliptic cohomology, in Advances in Homotopy theory, LMS Lect. Note Series 139, Cambridge Univ. Press, 1989, 87-104.
- [7] M. J. Hopkins, N. J. Kuhn, and D. C. Ravenel, Generalized group characters and complex oriented cohomology theories, Preprint, 1989.
- [8] M. J. Hopkins, N. J. Kuhn, D. C. Ravenel, Morave K-theories of classifying spaces and generalized characters for finite groups, in Algebraic Topolygy-Homotopy and Group Cohomology, Lect. Notes in Math. 1509, Springer, 1992, 186-209.
- [9] N. M. Katz, *p*-adic properties of modular schemes and modular forms, in Modular Functions of One Variable III, Lect. Notes in Math. 350, Springer, 1973, 69-190.
- [10] N. M. Katz, p-adic interpolation of real analytic Eisenstein series, Ann. of Math., 104 (1976), 459-571.
- P. S. Landweber (ed.), Elliptic Curves and Modular Forms in Algebraic Topology, Lect. Notes in Math. 1326, Springer, 1988.
- [12] G. Mason, Finite groups and modular functions, Proc. Symp. in Pure Math., 47 (Part I) (1987), 181-210.
- [13] H. R. Miller, The elliptic character and the Witten genus, Contemp. Math., 96 (1989), 281-289.
- [14] S. P. Norton, Generalized moonshine, Appendix to [12].
- [15] G. Segal, Elliptic cohomology, Seminaire Bourbaki 695 (1988), 187-201.
- [16] J-P. Serre, Formes modulaires et fonction zeta p-adique, in Modular Functions of One Variable III, Lect. Notes in Math. 350, Springer, 1973, 191-268.
- [17] G. Shimura, Introduction to the Arithmetic Theory of Automorphic Functions, Princeton Univ. Press, 1971.
- [18] J. Silverman, The Arithmetic of Elliptic Curves, GTM 106, Springer, 1986.