On the construction of elliptic cohomology

Jens Franke

Max-Planck-Institut für Mathematik
Gottfried-Claren-Straße 26
D-5300 Bonn 3

Germany

MPI / 92-3

On the construction of elliptic cohomology

Jens Franke
Max-Planck-Institut für Mathematik
Gottfried-Claren-Straße 26
W-5300 Bonn 3, Germany

December 21, 1991

Dedicated to Prof. H. Koch on the occasion of his sixtieth birthday

1 Introduction

The aim this paper is to present a simplified proof of the existence of elliptic cohomology. Recall that elliptic cohomology is a cohomology theory constructed from complex cobordism as follows.

Consider the Jacobi quartic

$$y^2 = 1 - 2\delta x^2 + \varepsilon x^4 \tag{1}$$

over $\mathbf{Z}[\frac{1}{2}, \delta, \varepsilon]$. For $\varepsilon(\delta^2 - \varepsilon) \neq 0$, this curve can be compactified to an elliptic curve by adding two points at infinity. The group law of this elliptic curve will be written additively, with zero given by $\mathbf{0} = (0, 1)$. Then x is a formal parameter of the elliptic curve (1). The resulting formal group law is Euler's formal group law

$$F_{\delta,\varepsilon}(x, \tilde{x}) = \tfrac{x\tilde{y}+y\tilde{x}}{1-\varepsilon x^2\tilde{x}^2} \tag{2}$$
$$y = \sqrt{1 - 2\delta x^2 + \varepsilon x^4}, \tilde{y} = \sqrt{1 - 2\delta \tilde{x}^2 + \varepsilon \tilde{x}^4}.$$

It is easy to see that this formal group law has coefficients in $\mathbf{Z}[\frac{1}{2}, \varepsilon, \delta]$.

Recall also that there is a complex cobordism spectrum $\mathbf{MU}$, that there is a formal group law $F_{\mathbf{MU}}(x, \tilde{x})$ over the coefficient ring $\mathbf{MU}_*$, and that by a theorem of Quillen (cf. [Qui69] or the textbooks [Ada74, Part II], [Rav86, §4.1] for an approach based on on Milnor's calculation of $\mathbf{MU}_*$, and [Qui71] for a direct approach) the formal group law $F_{\mathbf{MU}}$ is a universal formal group law. Applied to Euler formal group law, this means that there is a unique ring homomorphism

$$\phi: \mathbf{MU}_* \to \mathbf{Z}[\frac{1}{2}, \delta, \varepsilon] \tag{3}$$

which maps the coefficients of $F_M U$ to the coefficients of $F_{\delta,\varepsilon}$. This is a graded homomorphism if the grading on $\mathbf{Z}[\frac{1}{2},\varepsilon,\delta]$ is given by

$$\deg\delta = 4,\ \deg\varepsilon = 8. \tag{4}$$

We can now formulate the main theorem about the existence of elliptic cohomology, due to Landweber, Ravenel and Stong.

Theorem 1 *Let $P(\delta,\varepsilon)$ be a homogeneous polynomial of positive degree with respect to the grading (4). Then the functor from the stable homotopy category to graded vector spaces*

$$\mathbf{Ell}_{P*}X = \mathbf{MU}_*X \bigotimes_{\mathbf{MU}_*} \mathbf{Z}[\tfrac{1}{2},\delta,\varepsilon,P(\delta,\varepsilon)^{-1}], \tag{5}$$

where the second factor of the tensor product is an $\mathbf{MU}_*$-module by the map ϕ (3), is a generalised homology theory. Moreover, for finite spectra X, the associated cohomology theory is given by

$$\mathbf{Ell}_P^*X = \mathbf{MU}^*X \bigotimes_{\mathbf{MU}^*} \mathbf{Z}[\tfrac{1}{2},\delta,\varepsilon,P(\delta,\varepsilon)^{-1}], \tag{6}$$

where this time the grading on $\mathbf{Z}[\delta,\varepsilon]$ is the opposite of (4), i.e., $\deg\delta = -4$, $\deg\varepsilon = -8$. Moreover, the isomorphism (5) defines the elliptic homology spectrum $\mathbf{Ell}_P$ uniquely up to unique isomorphism in the stable homotopy category, and the multiplication on (6) for a finite CW-complex X, which is given by the ring structures of $\mathbf{MU}^*X$ and $\mathbf{Z}[\frac{1}{2},\delta,\varepsilon,P(\delta,\varepsilon)^{-1}]$, comes from a unique structure of a commutative ring spectrum on $\mathbf{Ell}_P$.

This cohomology theory is related to interesting geometric problems studied by Witten, Ochanine, Landweber, Stong, Bott, Taubes, Hirzebruch, Kreck, and Stolz (cf. [Seg88] and [KS91]). Unfortunately, the present paper is not concerned with these problems, but only with the algebraic construction of elliptic cohomology from complex cobordism.

The preprint [LRS] is unpublished, but a proof of theorem 1 (but without the subtle points of uniqueness and the structure of a ring spectrum) appears in [Lan88a], where it is based on certain congruences for the coefficients of the power series for multiplication by a prime p in the formal group $F_{\delta,\varepsilon}$. We can offer no fundamental new insight, but a significant simplification of the argument and a precise description of the situation in which it can be applied. As in [LRS] and [Lan88a], the construction is based on a verification of the conditions of Landweber's exact functor theorem for ϕ. However, the use of the difficult Chudnovsky-Landweber congruences can be avoided, since the assumptions of the Landweber exact functor theorem are easy consequences of the result of Deuring and Eichler (which is also used in the proof of the congruences) that

the height of the formal group law of an elliptic curve in positive characteristic is never bigger than two. This fact was also noticed by Baker [Bak90, Proof of theorem 1], but without giving details.

We also discuss the rather subtle question about the uniqueness and the existence a ring structure on a spectrum obtained by the Landweber exact functor theorem for a countable $\mathbf{MU}_*$-algebra.

The organisation of this paper is as follows. In section 2, we prove theorem 1 by verifying the Landweber conditions for Euler's formal group law. This proves theorem 1 up to the questions about uniqueness and the ring structure. These questions are settled in section 3 for general spectra obtained by the exact functor theorem from countable $\mathbf{MU}_*$-modules or algebras. In section 4, we explain under which conditions other families of elliptic curves satisfy the Landweber conditions. We apply this to Hirzebruch's elliptic genera, which have values in the ring of modular forms modulo $\Gamma_1[N]$. In section 5, we give a simple proof of the Chudnovsky-Landweber congruences. We tried to keep sections 2 and 5 as elementary as we could. Due to their general nature, sections 3 and 4 are more abstract. The reader who is only interested in the congruences may go directly to section 5.

This paper is based on the author's talk at the 1991 Geyer-Harder workshop on elliptic cohomology in Oberwolfach, which was organised by M. Kreck, W. Nahm and S. Ochanine. The author is indebted to the audience of this workshop for interesting discussions, in particular to M. Kreck, U. Jannsen, and R. Jung for recommending him to publish his talk, and also to D. Husemoller and F. Waldhausen, for teaching him stable homotopy. He also had an interesting conversation with G. Laumon about parts of section 4.

2 Verification of the Landweber conditions for the Jacobi quartic

Let M_* be a graded $\mathbf{MU}_*$-module. To verify that the functor on the stable homotopy category defined by

$$\mathbf{E}_{M*}X = \mathbf{MU}_*X \bigotimes_{\mathbf{MU}_*} M_* \tag{7}$$

is a generalised homology theory, one has to check that the long exact sequences of bordism groups defined by a cofibration sequence of topological spaces (or, equivalently, by exact triangles in the stable homotopy category). For instance, this could be ensured by the assumption that M is flat over $\mathbf{MU}_*$. By using the Landweber-Novikov cooperations on complex bordism, it is however possible to work with the weaker Landweber conditions, which we now describe.

Consider a prime p, and let $[p]_F$ be the power series for multiplication by p

in the formal group F, i.e.,

$$\begin{aligned} [1]_F &= X \\ [n]_F &= F([n-1]_F, X). \end{aligned}$$

Let u_k be the coefficient of X^{p^k} in the formal power series $[p]_F$. The dependence of u_k on p and F will not be expressed in the subscript, because we will usually think of a fixed prime p and a fixed formal group law F. We can now formulate the Landweber exact functor theorem, cf. [Lan76]. In the case of the universal formal group law $F_{\mathbf{MU}}$, this gives us elements $p, u_1, \ldots \in \mathbf{MU}_*$.

Theorem 2 *Let M_* be a graded $\mathbf{MU}_*$-module such that for each prime p, the sequence of elements in $\mathbf{MU}_*$ $(p, u_1, u_2, \ldots)$ is M-regular, i.e., that multiplication by u_k in $M/(p, u_1, \ldots, u_{k-1})M$ is injective.*

A. *Then the functor defined by (7) on the category of spectra is a generalised homology theory. Moreover, for finite spectra X its associated cohomology theory is given by*

$$M^* \bigotimes_{\mathbf{MU}^*} \mathbf{MU}^* X, \tag{8}$$

where M^* is M_* with its opposite grading, i.e., $M^k = M_{-k}$.

B. *We have*

$$\mathrm{Tor}_1^{\mathbf{MU}_*}(M_*, N_*) = 0 \tag{9}$$

for any $\mathbf{MU}_*$-module N_* which admits the structure of an $\mathbf{MU}_*\mathbf{MU}$-comodule.

Indeed, by the exactness theorem [Lan76, Theorem 2.6] and by the Adams-Brown representability theorem [Swi75, Theorem 9.27], (8) on the category of finite spectra is representable by a spectrum $\mathbf{E}_M$. Using the Spanier-Whitehead duality operator D, we have by applying [Ada74, Remark 5.3 and Lemma 5.5] (where DX was denoted X^*) twice

$$\mathbf{E}_{M*}X = \mathbf{E}_M^{-*}DX = M^{-*} \bigotimes_{MU^{-*}} \mathbf{MU}^{-*}DX = M_* \bigotimes_{\mathbf{MU}_*} \mathbf{MU}_* X.$$

Since both sides commute with filtered inductive limits, this also holds for infinite spectra, verifying (7). In the next section, we will discuss some subtle questions of this construction, for instance the question if $\mathbf{E}_M$ is determined uniquely up to unique isomorphism in the stable homotopy category and if it has the structure of a ring spectrum. The reader can for the moment skip the following remarks about (9) since they are only needed in the next section. If N is a $\mathbf{MU}_*\mathbf{MU}$-comodule which is finitely presented as a $\mathbf{MU}_*$-module, (9) is contained in the proof of [Lan76, Theorem 2.6]. To get the vanishing in general, one uses a result of Miller and Ravenel, which says that any $\mathbf{MU}_*\mathbf{MU}$-comodule is

the filtered inductive limit of a family of finitely presented $\mathbf{MU}_*\mathbf{MU}$-comodules. This is proved in the **BP**-case in [MR77, Lemma 2.11]. The proof given there also works for **MU**.

Let R_* be a graded ring and F a formal group law over R such that F has total degree -2, defining a homomorphism $\phi_F\colon \mathbf{MU}_* \to R_*$. To verify the Landweber conditions for the $\mathbf{MU}_*$-module R_*, we have to verify that for any prime p the sequence $(p, u_1, \ldots)$ is regular in R, i.e., that u_k is no zero divisor in $R/(p, u_1, \ldots, u_{k-1})R$. To prove the Landweber-Ravenel-Stong theorem 1, we have to verify these conditions for $R = \mathbf{Z}[\frac{1}{2}, \delta, \varepsilon, P(\delta, \varepsilon)^{-1}]$, where P is homogeneous of positive degree with respect to (4). We will fix an odd prime number p and verify the following conditions, which imply the assumption of theorem 2:

1. p is no zero divisor in R.
2. $u_1(\delta, \varepsilon)$ does not identically vanish modulo p.
3. $u_2(\delta, \varepsilon)$ is invertible modulo the ideal (p, u_1).

The first of these points is clear. To verify 2, let us consider the singular cases $\varepsilon = \delta^2$ and $\varepsilon = 0$. If $\varepsilon = \delta^2$, we have

$$\lambda\big(F(x, \tilde{x})\big) = \lambda(x)\lambda(\tilde{x}).$$

with

$$\lambda(x) = \frac{1 - \sqrt{\delta}x}{1 + \sqrt{\delta}x}$$

In other words, λ defines a homomorphism from $F_{\delta,\varepsilon}$ to the multiplicative formal group law. Since $u_1 = 1$ for the multiplicative formal group law, we have

$$u_1 \equiv \lambda'(0)^{p-1} \equiv \delta^{\frac{p-1}{2}} \pmod{(p, \delta^2 - \varepsilon)}. \tag{10}$$

If $\varepsilon = 0$, we have an isomorphism between $F_{\delta,\varepsilon}$ and the multiplicative formal group law defined by

$$\lambda(x) = \sqrt{-2\delta}x + \sqrt{1 - 2\delta x^2},$$

hence

$$u_1 \equiv \lambda'(0)^{p-1} \equiv (-2\delta)^{\frac{p-1}{2}} \pmod{(p, \varepsilon)} \tag{11}$$

Each of (10) or (11) implies that $u_1(\delta, \varepsilon)$ does not vanish identically modulo p, establishing the second point.

To establish the third point, we need a classical result of Eichler and Deuring about the height of the formal group law of an elliptic curve. Recall that the height of a formal group law F over a field of characteristic p is the smallest k such that $u_k \neq 0$, or infinity if the power series $[p]_F$ vanishes identically. The theorem which we need is the following:

Theorem 3 *If $\mathcal{E}$ is an elliptic curve over a field of positive characteristic and if x is a rational function on $\mathcal{E}$ with $x(0) = 0$ and $d_0 x \neq 0$, then the height of the formal group law defined by $F(x(P), x(Q)) = x(P+Q)$ is either one or two.*

A proof can be found in [Sil86, Corollary IV.7.5.] or in [Hus87, §13]. The theorem also follows from the fact the the isogeny of multiplication by p on an elliptic curve has degree p^2, cf. [Mum88, Proposition at the end of §II.6] or [KM85, Theorem 2.3.1].

Now if for the Euler formal group law u_2 was not invertible in $R/(p, u_1)$, then there would be a maximal ideal $\mathfrak{p} \subset R$ which contains p, u_1, and u_2. If $\mathfrak{p}$ would contain $\varepsilon(\delta^2 - \varepsilon)$, then it would contain both ε and δ by (10) or (11), since it contains u_1. But then $\mathfrak{p}$ would contain P,[1] which is impossible since by definition P is a unit in R. It follows that $\varepsilon(\delta^2 - \varepsilon) \neq 0$ in the residue field $k = R/\mathfrak{p}$, hence the Jacobi quartic

$$y^2 = 1 - 2\delta x^2 + \varepsilon x^4$$

is known to be [Hus87, §4.3] an open subset of an elliptic curve $\mathcal{E}$ over k with $\mathbf{0} = (0, 0)$. It is also known that the Euler formal group law $F_{\delta,\varepsilon}$ is the formal group law defined by this elliptic curve and the local parameter x, cf. for instance the appendix to [Lan88c]. Since $\mathfrak{p}$ contains p, u_1 and u_2, it follows that the height of the formal group law defined by $\mathcal{E}$ is bigger than two. This contradiction to theorem 3 proves the invertibility of $u_2 \pmod{(p, u_1)}$ and completes the proof of theorem 1.

3 Uniqueness for the exact functor construction

It remains to prove the uniqueness claim and the claim about the existence of a ring structure in theorem 2. Our methods work for arbitrary countable $\mathbf{MU}_*$-modules which satisfy the Landweber conditions. Although we will only formulate the results for $\mathbf{MU}$, they are also valid for $\mathbf{BP}$. In the $\mathbf{BP}$-case, similar uniqueness questions for v_n^{-1} have been investigated by Yosimura in [Yos88]. I does not seem to be easy to use this method in the case of elliptic cohomology. A discussion of some other cases can be found at the end of the second section of [Rav84], which also uses the methods of Yosimura. Our approach will be completely different and gives a weaker result, but works for arbitrary countable spectra obtained by the Landweber construction.

We first have to introduce some notations and conventions, which will we will use throughout this section. $\mathbf{MU}_*\mathbf{MU}$ is the module of cooperations on $\mathbf{MU}$. The pair $(\mathbf{MU}_*, \mathbf{MU}_*\mathbf{MU})$ comes with various structure maps, which are easily

[1] This is the only point where we have used the fact that P is homogeneous of positive degree. Actually, only the fact that $P(0,0) = 0$ was used, but homogeneity is necessary to get a grading on R.

memorised by saying that this pair forms a cogroupoid object in the category of rings. In particular, there are cosource and cotarget maps $\mathbf{MU}_* \to \mathbf{MU}_*\mathbf{MU}$, a coidentity $\mathbf{MU}_*\mathbf{MU} \to \mathbf{MU}_*$, and a cocomposition $\mathbf{MU}_*\mathbf{MU} \otimes \mathbf{MU}_*\mathbf{MU} \to \mathbf{MU}_*\mathbf{MU}$. Unless otherwise specified, tensor products, and torsion products in this section are over $\mathbf{MU}_*$. The tensor product $\mathbf{MU}_*\mathbf{MU} \otimes M_*$ will always be defined using the structure of a $\mathbf{MU}_*$-modules on $\mathbf{MU}_*\mathbf{MU}$ given by the cotarget map, and will be given the structure of a $\mathbf{MU}_*$-module using the cosource map. For $M_* \otimes \mathbf{MU}_*\mathbf{MU}$, the opposite conventions apply. It is known that $\mathbf{MU}_*\mathbf{MU}$ is a free $\mathbf{MU}_*$-module in both ways, and that $\mathbf{MU}_*(\mathbf{MU} \wedge X) \cong \mathbf{MU}_*\mathbf{MU} \otimes \mathbf{MU}_* X$. A $\mathbf{MU}_*\mathbf{MU}$-comodule is a $\mathbf{MU}_*$-module M_* which comes with a map $M_* \to \mathbf{MU}_*\mathbf{MU} \otimes M_*$ satisfying all sorts of compatibilities. For instance, complex bordism of a spectrum is a $\mathbf{MU}_*\mathbf{MU}$-comodule. For a discussion of these question, we refer to [Ada74, Part III, 12–15] or to [Rav86, §2.2].

For an integer k, let

$$\pi(k) = \begin{cases} 0 & \text{if } k \text{ is odd} \\ 1 & \text{if } k \text{ is even} \end{cases}$$

be its parity.

Theorem 4 *Let L_*, M_*, N_* be countable $\mathbf{MU}_*$-modules which are concentrated in even dimension, and which satisfy the conditions of Landweber's exact functor theorem 2.*

A. *The spectrum $\mathbf{E}_M$ is characterised by the isomorphism (7) uniquely up to unique isomorphism in the stable homotopy category. Moreover, the natural transformation*

$$\mathbf{E}_{M*}X \otimes \mathbf{MU}_*Y \to \mathbf{E}_{M*}(X \wedge Y)$$

defined by (7), and the ring structure on $\mathbf{MU}$ comes from a unique structure of a $\mathbf{MU}$-module spectrum on $\mathbf{E}_M$.

B. *There is a spectral sequence of $\mathbf{MU}_*$-modules*

$$E_2^{p,q} = \mathrm{Ext}^{p,q}_{\mathbf{MU}_*}(\mathbf{MU}_*X, M_*) \Rightarrow \mathbf{E}^{p+q}_{M*}X \tag{12}$$

for any spectrum X. Here $\mathrm{Ext}^{p,q}$ is the graded object Ext^p, and the convergence properties of the spectral sequence are as described in [Ada74, Theorem III.8.2].

C. *We have a canonical isomorphism*

$$[\mathbf{E}_M, \Sigma^k \mathbf{E}_N] \cong \mathrm{Ext}^{\pi(k),k-\pi(k)}_{\mathbf{MU}_*}(\mathbf{MU}_*\mathbf{MU} \otimes M_*, N_*). \tag{13}$$

Recall our convention that the tensor product is over $\mathbf{MU}_*$, and that $\mathbf{MU}_*\mathbf{MU} \otimes M_*$ is always defined using the structure of a $\mathbf{MU}_*$-modules on $\mathbf{MU}_*\mathbf{MU}$ given by the cotarget map, and is given the structure of a $\mathbf{MU}_*$-module using the cosource map.

D. *If a map $\mathbf{E}_M \to \mathbf{E}_N$ of even degree induces the zero map $\mathbf{E}_{M*}X \to \mathbf{E}_{N*}X$ for any finite spectrum X, then it is homotopic to zero. However, a map $\mathbf{E}_M \to \mathbf{E}_N$ of odd degree always induces the zero map on homology, or on the cohomology of any finite spectrum.*

E. *Let two maps of even degree $\mathbf{E}_L \to \mathbf{E}_M$ and $\mathbf{E}_M \to \mathbf{E}_N$ be given by*

$$\phi: \mathbf{MU}_*\mathbf{MU} \otimes L_* \to M_*$$

and

$$\psi: \mathbf{MU}_*\mathbf{MU} \otimes M_* \to N_*$$

in (13). Then their composition is given by

$$\begin{aligned} \mathbf{MU}_*\mathbf{MU} \otimes L_* &\xrightarrow{\text{cocomposition}} \mathbf{MU}_*\mathbf{MU} \otimes \mathbf{MU}_*\mathbf{MU} \otimes L_* \\ &\xrightarrow{\mathrm{Id} \otimes \phi} \mathbf{MU}_*\mathbf{MU} \otimes M_* \\ &\xrightarrow{\psi} N_*. \end{aligned}$$

The composition of maps of odd and even degree is given in the same way, where one of the maps ϕ ore ψ is now an extension class. The composition of two maps of odd degree is homotopic to zero.

F. *A map $\mathbf{E}_M \to \mathbf{E}_N$ is a map of* **MU***-module spectra if its image by 13 lies in the image of the map*

$$\mathrm{Ext}^{\pi(k),k-\pi(k)}(M_*, N_*) \to \mathrm{Ext}^{\pi(k),k-\pi(k)}(\mathbf{MU}_*\mathbf{MU} \otimes M_*, N_*) \qquad (14)$$

defined by the coidentity on $\mathbf{MU}_*\mathbf{MU}$. If k is even or if M_* admits the structure of a $\mathbf{MU}_*\mathbf{MU}$-comodule, then the map (14) is injective, and its image consists of all maps $\mathbf{E}_M \to \mathbf{E}_N$ of **MU***-module spectra.*

Proof: It is easy to see that $\mathbf{E}_M$ is unique up to isomorphism. Indeed, using the countability of its homotopy groups, one can see that any spectrum which satisfies the condition for $\mathbf{E}_M$ has a countable subspectrum to which it is homotopy equivalent. Let $\mathbf{E}_M$ and $\tilde{\mathbf{E}}_M$ be two spectra with this property. Then for any finite subspectrum $X \subset \mathbf{E}_M$, the inclusion defines a cohomology class in

$$\mathbf{E}_M^* X \cong M^* \otimes \mathbf{MU}^* X \cong \tilde{\mathbf{E}}_M^* X.$$

We get a consistent system of maps from the finite subspectra of $\mathbf{E}_M$ to $\tilde{\mathbf{E}}_M$. By the Milnor exact sequence [Ada74, Proposition III.8.1], these maps come from a homotopy class $\mathbf{E}_M \to \tilde{\mathbf{E}}_M$ which induces an isomorphism on homology. Hence it induces an isomorphism on homotopy groups and is a homotopy equivalence. However, its uniqueness is a question about a $\varprojlim^1$-term, which is the hard part of the theorem. The uniqueness will follow once we have established part **D.**.

The crucial point will be the spectral sequence (12), which will eventually follow from [Ada74, Theorem III.13.6]. However, we can not yet apply this result since we do not yet know for sure that $\mathbf{E}_{M_*}$ is a $\mathbf{MU}$-module spectrum. However, it is possible to get Adam's machinery to work under a weaker assumption.

Lemma 1 *Let E be a ring spectrum and let F be any spectrum, and assume that we are given the structure of a E_*-module on F_* and a E_*-linear map $E_*F \to F_*$. These two data give us a homomorphism*

$$F^*X \to \mathrm{Hom}_{E_*}(E_*X, F_*) \tag{15}$$

which is functorial in X. Suppose that the following two conditions hold.

Y *E is the direct limit of subspectra E_α for which $E_*(DE_\alpha)$ is a projective E_*-module and for which (15) is an isomorphism.*

Z *If X is any spectrum with $E_*X = \{0\}$, then F_*X and F^*X vanish. Then we have a spectral sequence of groups*

$$E_2^{p,q} = \mathrm{Ext}_{E_*}^{p,q}(E_*X, F_*) \Rightarrow F^{p+q}X$$

with the convergence properties as in [Ada74, Theorem III.8.2]. Moreover, the map $F^*X \to E_2^{0,*}$ is (15).

Indeed, the assumptions of the lemma are all that is needed to carry out the proof of [Ada74, Theorem III.13.6] if one does not need the differentials of the spectral sequence to be homomorphisms of E_*-modules.

We want to apply the lemma to $E = \mathbf{MU}$ and $F = \mathbf{E}_M$. Then F_* is the $\mathbf{MU}_*$-modules M_*, and $F_*E = \mathbf{MU}_*\mathbf{MU} \otimes M_* \to M_*$ by the coidentity and the $\mathbf{MU}_*$-module structure on M_*. Condition **Y.** follows from [Ada74, III.13.4.] and (8). To verify condition **Z.**, consider the transformation

$$\begin{aligned}(\mathbf{MU} \wedge \mathbf{E}_M)_*X &= \mathbf{E}_{M*}(\mathbf{MU} \wedge X) \\ &= M \otimes \mathbf{MU}_*\mathbf{MU} \otimes \mathbf{MU}_*X \\ &\to M_* \otimes \mathbf{MU}_*X \\ &= \mathbf{E}_M X,\end{aligned} \tag{16}$$

where the non-isomorphic arrow is given by the coidentity. By the arguments used to prove the uniqueness of $\mathbf{E}_M$, this natural transformation comes from a (possibly non-unique) map $f\colon \mathbf{MU} \wedge \mathbf{E}_M \to \mathbf{E}_M$. When composing f with the map $g\colon \mathbf{E} \to \mathbf{MU} \wedge \mathbf{E}$ defined by the identity of $\mathbf{MU}$, we get the identity transformation on homology, hence on homotopy groups. Replacing f by $(fg)^{-1}f$ if necessary, we may assume $fg = \mathrm{Id}$. This means that every map $X \to \mathbf{E}_M$ factorises over $\mathbf{MU} \wedge X$ and proves the vanishing of E_M^*X if $\mathbf{MU}_*X$ vanishes. The other assertion of **Z.** follows directly from (7).

We now have (12) available, at least as a spectral sequence of groups. The isomorphism (13), at least as an isomorphism of groups, follows from this and the following algebraic lemma:

Lemma 2 *If M_* is a $\mathbf{MU}_*$-module which satisfies the assumptions of the exact functor theorem. Then $\mathbf{MU}_*\mathbf{MU} \otimes M_*$ is a flat $\mathbf{MU}_*$ module. If in addition M_* is countable, then*

$$\mathrm{Ext}^{p,*}_{\mathbf{MU}_*}(\mathbf{MU}_*\mathbf{MU} \otimes M_*, N_*)$$

vanishes for $p > 1$ and any $\mathbf{MU}_*$-module N_*.

To get the flatness assertion, note that

$$\mathrm{Tor}_1(N_*, \mathbf{MU}_*\mathbf{MU} \otimes M_*) = \mathrm{Tor}_1(N_* \otimes \mathbf{MU}_*\mathbf{MU}, M_*)$$

by the flatness of $\mathbf{MU}_*\mathbf{MU}$. The left hand side vanishes by part **B.** of (2), since $N_* \otimes \mathbf{MU}_*\mathbf{MU}$ admits the structure of a $\mathbf{MU}_*\mathbf{MU}$-comodule given by the cocomposition on $\mathbf{MU}_*\mathbf{MU}$.

To get the vanishing of the Ext-groups, we apply the following lemma.

Lemma 3 *If A is a countable flat module over a countable ring R, then M has a free resolvent of length two.*

To prove lemma 3, we use a result of D. Lazard [Laz64], which says that a flat module is the filtered inductive limit of free modules. We want to make sure that in our case the limit can be chosen to be indexed by the natural numbers. Let G be the free module generated by the elements of A, and let $f: G \to A$ be the canonical map. Let X_i be finitely generated free submodules of G and Y_i finitely generated submodules of $X_i \cap \ker f$ such that $X_i \subset X_{i+1}$, $Y_i \subset Y_{i+1}$, $G = \bigcup_{i=1}^{\infty} X_i$, $\ker f = \bigcup_{i=1}^{\infty} Y_i$. By [Laz64, Théorème 1], the map $X_i/Y_i \to A$ factorises over a map $f_i: F_i \to A$ from a finitely generated free module. Since the image of f_i is contained in that of X_j in A for some $j \leq i$, we may chose a cofinal sequence i_k of integers morphisms $t_k: F_{i_k} \to F_{i_{k+1}}$ over A. Then A is the limit of the F_{i_k}, which is the cokernel of the injective map of free modules

$$\begin{array}{ccc} \coprod_{i=1}^{\infty} F_{i_k} & \to & \coprod_{i=1}^{\infty} F_{i_k} \\ (f_k)_{k=0}^{\infty} & \to & (f_k - t_{k-1}(f_{k-1}))_{k=0}^{\infty} \end{array}$$

where $t_0 = 0$. This completes the proof of lemma 3 and also the proof of lemma 2.

We now have (13) as an isomorphism of groups. By the last assertion of lemma 1, the image of a map of even degree $f: \mathbf{E}_M \to \mathbf{E}_N$ can be reconstructed from the map

$$\mathbf{E}_{M*}\mathbf{MU} \to \mathbf{E}_{N*}\mathbf{MU}$$

which it induces. If f vanishes on the homology of any finite spectrum, then it also vanishes on the homology of $\mathbf{MU}$ since homology commutes with filtered inductive limits. But then the image of f by (13) is zero, hence f vanishes. This proves the assertion of **D.** about morphisms of even degree. As we mentioned at the beginning of the proof, this also proves that $\mathbf{E}_M$ is unique up to unique isomorphism. To get the structure of a $\mathbf{MU}$-module spectrum, recall that we have a map $\mathbf{MU} \wedge \mathbf{E}_M \to \mathbf{E}_M$ which induces (16) on homology. Since $\mathbf{MU} \wedge \mathbf{E}_M = \mathbf{E}_{\mathbf{MU}_*\mathbf{MU} \otimes M_*}$ and by the flatness of $\mathbf{MU}_*\mathbf{MU} \otimes M_*$ proved lemma 2, the part of **D.** which is already proved implies the uniqueness of this map. A similar uniqueness argument can be used to verify the axioms of a $\mathbf{MU}$-module spectrum. This completes the proof of **A.**. Since the other parts of the theorem will not be needed for our treatment of elliptic cohomology, the rest of the proof will be rather terse.

Now we can deduce **B.** in full glory from [Ada74, §III.13]. This implies that (13) is an isomorphism of $\mathbf{MU}_*$-modules and completes the proof of **C.** To verify the remaining part of **D.**, we first need the following lemma:

Lemma 4 *If the image of $f: X \to \mathbf{E}_M$ in the $E_2^{0,*}$-term of (12) is denoted by ϕ, then the map $\mathbf{MU}_*X \to \mathbf{MU}_*\mathbf{E}_M$ induced by ϕ is given by*

$$\mathbf{MU}_*X \to \mathbf{MU}_*\mathbf{MU} \otimes \mathbf{MU}_*X \xrightarrow{\mathrm{Id} \otimes \phi} \mathbf{MU}_*\mathbf{MU} \otimes M_* = \mathbf{MU}_*\mathbf{E}_M, \quad (17)$$

where the left arrow is the coaction of $\mathbf{MU}_*\mathbf{MU}$ on $\mathbf{MU}_*X$.

This is easily verified. In **D.**, we conclude that for a map $f: \mathbf{E}_M \to \mathbf{E}_N$ of odd degree the induced map $\mathbf{MU}_*\mathbf{E}_M \to \mathbf{MU}_*\mathbf{E}_N$ is zero. By the isomorphism $\mathbf{E}_{M*}X \cong \mathbf{MU}_*X \otimes \mathbf{MU}_*\mathbf{E}_M$ and the analogous isomorphism for N_*, it follows that f induces the zero map on the homology of $\mathbf{MU} \wedge X$. By the injectivity of the map $\mathbf{E}_{N*}X \to \mathbf{E}_{N*}\mathbf{MU} \wedge X$ (existence of a $\mathbf{MU}$-module structure for $\mathbf{E}_N$), this also implies the vanishing of the map which f induces on the homology of X, and completes the proof of **D.**.

Now we consider **E.**, which is concerned with the behaviour of the composition of maps $\mathbf{E}_L \xrightarrow{f} \mathbf{E}_M \xrightarrow{g} \mathbf{E}_N$. If f is of even degree, our formula follows from the fact that the spectral sequence (12) is functorial in X and from formula (17). If the degree of g is even, one easily checks how the spectral sequence [Ada74, Theorem III.13.6] behaves with respect to (possibly non-linear) maps of module spectra. If both g and f are of odd degree, their composition is of even degree and induces zero on homology, hence it vanishes.

The fact that a map $\mathbf{E}_M \to \mathbf{E}_N$ is a map of $\mathbf{MU}$-module spectra can be expressed as the commutativity of a certain diagram, which can be examined by the composition formula of **E.**. One sees easily that the map $\mathbf{MU} \wedge \mathbf{E}_M \to \mathbf{E}_N$ which defines the structure of a $\mathbf{MU}$-module spectrum on $\mathbf{E}_M$ corresponds by (13) to the map

$$\begin{aligned} \mathbf{MU}_*\mathbf{MU} \otimes \mathbf{MU}_*\mathbf{MU} \otimes M_* &\to M_* \\ c_1 \otimes c_2 \otimes m &\to \nu(c_1)\nu(c_2)m, \end{aligned} \quad (18)$$

where $\nu: \mathbf{MU}_*\mathbf{MU} \to \mathbf{MU}_*$ is the coidentity. Using this, we see that a map $f: \mathbf{E}_M \to \mathbf{E}_N$ with image ϕ under (13) is a $\mathbf{MU}$-module morphism if and only if the diagram

$$\begin{array}{ccc}
\mathbf{MU}_*\mathbf{MU} \otimes \mathbf{MU}_*\mathbf{MU} \otimes M_* & & \\
\downarrow{\scriptstyle \mu \otimes \mathrm{Id} \otimes \mathrm{Id}} & & \\
\mathbf{MU}_*\mathbf{MU} \otimes \mathbf{MU}_*\mathbf{MU} \otimes \mathbf{MU}_*\mathbf{MU} \otimes M_* & \xrightarrow{\mathrm{Id} \otimes (18)} & \mathbf{MU}_*\mathbf{MU} \otimes M_* \\
\downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \phi} \\
\mathbf{MU}_*\mathbf{MU} \otimes \mathbf{MU}_*\mathbf{MU} \otimes N_* & \xrightarrow[(18)]{} & N_*
\end{array}$$

commutes. For the sake of simplicity, we describe the arrows in this diagram, in the case where ϕ is a homomorphism. If ϕ is an extension class, the definition is similar. The map μ is the cocomposition map on $\mathbf{MU}_*\mathbf{MU}$, and α is defined by

$$\alpha(c_1 \otimes c_2 \otimes c_3 \otimes m) = c_1 \otimes \left(\sum \nu(c_2) c'_{3,i} \phi(c''_{3,i} \otimes m)\right),$$

where $\mu(c_3) = \sum c'_{3,i} \otimes c''_{3,i}$. It follows that an element $c_1 \otimes c_2 \otimes m$ in the upper corner of the diagram is mapped to $\phi(c_1\nu(c_2) \otimes m)$ in the right lower corner by the composition of the arrows via the right middle corner, and to $\phi(\nu(c_1)c_2 \otimes m)$ by the composition of the arrows via the left lower corner. It follows that f is a morphism of $\mathbf{MU}$-module spectra if and only if ϕ is in the kernel of the map

$$\begin{aligned}
&\mathrm{Ext}^{\pi(k),k-\pi(k)}(\mathbf{MU}_*\mathbf{MU} \otimes M_*, N_*) \to \\
&\quad \to \mathrm{Ext}^{\pi(k),k-\pi(k)}(\mathbf{MU}_*\mathbf{MU} \otimes \mathbf{MU}_*\mathbf{MU} \otimes M_*, N_*)
\end{aligned}$$

defined by

$$\begin{aligned}
\beta: \mathbf{MU}_*\mathbf{MU} \otimes \mathbf{MU}_*\mathbf{MU} &\to \mathbf{MU}_*\mathbf{MU} \\
c_1 \otimes c_2 &\to c_1\nu(c_2) - \nu(c_1)c_2.
\end{aligned}$$

But β is a surjection onto the kernel $\mathbf{MU}_*\mathbf{MU}^\circ$ of $\nu: \mathbf{MU}_*\mathbf{MU} \to \mathbf{MU}_*$, which is ($\mathbf{MU}_*$-nonlinearly) split by the map

$$\begin{aligned}
\mathbf{MU}_*\mathbf{MU}^\circ &\to \mathbf{MU}_*\mathbf{MU} \otimes \mathbf{MU}_*\mathbf{MU} \\
c &\to c \otimes 1.
\end{aligned}$$

Therefore, ϕ comes from a map of **MU**-module spectra if its restriction to $\mathbf{MU}_*\mathbf{MU}^o \otimes M_*$ vanishes, and this condition is is also necessary if ϕ is a homomorphism. If M_* admits the structure of a $\mathbf{MU}_*\mathbf{MU}$-comodule $\mu_M: M_* \to \mathbf{MU}_*\mathbf{MU} \otimes M_*$, then the map $\beta \otimes \mathrm{Id}_M$ has a linear splitting

$$\begin{aligned} \mathbf{MU}_*\mathbf{MU}^o \otimes M_* &\to \mathbf{MU}_*\mathbf{MU} \otimes \mathbf{MU}_*\mathbf{MU} \otimes M_* \\ c \otimes m &\to c \otimes \mu_M(m), \end{aligned}$$

hence in this case the vanishing of the restriction of ϕ to $\mathbf{MU}_*\mathbf{MU}^o \otimes M_*$ also is a necessary condition for ϕ to define a homomorphism of **MU**-module spectra. But the restriction of ϕ to $\mathbf{MU}_*\mathbf{MU}^o \otimes M_*$ is zero if and only if ϕ is in the image of (14). In the case of maps of even degree, (14) is clearly injective on homomorphisms. In the case of extensions, it is at least injective if M_* has the structure of a $\mathbf{MU}_*\mathbf{MU}$-comodule, since μ_M defines a splitting. **Q.E.D.**

If M_* has components of both odd and even degree, then we shall see below that $\mathbf{E}_M$ is no longer defined uniquely up to unique isomorphism by (7). However, it is still possible to make a canonical choice of $\mathbf{E}_M$ by

$$\mathbf{E}_M = \mathbf{E}_{M^{\mathrm{odd}}} \oplus \mathbf{E}_{M^{\mathrm{even}}},$$

where M_*^{even} and M_*^{odd} are the odd and the even components of M_*. By applying (13) to the components of odd and even degree, we obtain a canonical decomposition

$$[\mathbf{E}_M, \mathbf{E}_N] = \mathrm{Hom}_{\mathbf{MU}_*}(\mathbf{MU}_*\mathbf{MU} \otimes M_*, N_*) \oplus \mathrm{Ext}^{1,-1}(\mathbf{MU}_*\mathbf{MU} \otimes M_*, N_*) \tag{19}$$

of the group of morphisms from $\mathbf{E}_M$ to $\mathbf{E}_N$ in the stable homotopy category.

Let us also discuss the possibility of defining the structure of a ring spectrum.

Theorem 5 *Let R_* be a countable $\mathbf{MU}_*$-algebra with unit which satisfies the conditions of the Landweber exact functor theorem. Then we have natural transformations*

$$\begin{aligned} \mathbf{E}_{R*}X \otimes \mathbf{E}_{R*}X &\to \mathbf{E}_{R*}X \wedge X \\ \mathbf{MU}_*X &\to \mathbf{E}_{R*}X. \end{aligned} \tag{20}$$

*The first of these transformations is given by the $\mathbf{MU}_*$-algebra structure on R_* and by (7), the second transformation is given by (7) and the unit element of R_*. If R_* is concentrated in even degree, these transformations come from a unique structure of a **MU**-algebra spectrum on $\mathbf{E}_R$. Moreover, the **MU**-algebra spectrum $\mathbf{E}_R$ is commutative if R_* is commutative.*

*If R_* has components of both odd and even degree, then there is still a canonical way of defining the structure of a **MU**-algebra spectrum on $\mathbf{E}_R$, although its multiplication is no longer uniquely determined by (20). The map $\mathbf{MU} \to \mathbf{E}_R$ is always uniquely defined by the second transformation in (20).*

Proof: By the arguments used at the beginning of the proof of theorem 4, the transformations (20) come from maps

$$\begin{aligned} \mu\colon \mathbf{E}_R \wedge \mathbf{E}_R &\to \mathbf{E}_R \\ \iota\colon \mathbf{MU} &\to \mathbf{E}_R. \end{aligned}$$

We have $\mathbf{E}_R \to \mathbf{E}_R = \mathbf{E}_{R\otimes \mathbf{MU}_*\mathbf{MU}\otimes R}$, and $R_* \otimes \mathbf{MU}_*\mathbf{MU} \otimes R_*$ satisfies the conditions of the exact functor theorem, by the flatness part of lemma 2. Therefore, if R_* is concentrated in even degree, μ and ι are uniquely determined by their action on homology. By a similar uniqueness argument, the axioms for a **MU**-algebra structure are satisfied.

If R_* is no longer concentrated in even degree, one defines μ and ι by their image in (19), using the map

$$\mathbf{MU}_*\mathbf{MU} \otimes \mathbf{MU}_*\mathbf{MU} \otimes R_* \to R_*$$

defined by the coidentity on $\mathbf{MU}_*\mathbf{MU}$ and the $\mathbf{MU}_*$-algebra structure on R_* for μ, and the transformation

$$\mathbf{MU}_*\mathbf{MU} \otimes \mathbf{MU}_*\mathbf{MU} \to R_*$$

defined by the coidentity and the $\mathbf{MU}_*$-module structure on R_* for ι. The axioms of a **MU**-algebra structure are easily verified, using the composition formulas in theorem 4.**E**. **Q.E.D.**

To see that our precautions in the case of modules which have both odd and even components are really necessary, consider $\mathbf{MU}_\mathbf{Q} = \mathbf{E}_{\mathbf{MU}_*\bigotimes_\mathbf{Z}\mathbf{Q}}$. By (13), we have

$$[\mathbf{MU}_\mathbf{Q}, \Sigma^k\mathbf{MU}] = \begin{cases} \mathrm{Hom}^{k-1}_{\mathbf{MU}_*}\left(\mathbf{MU}_*\mathbf{MU}, \mathbf{MU}_*\bigotimes_\mathbf{Z}(\hat{\mathbf{Z}}/\mathbf{Z})\right) & \text{if } k \text{ is odd} \\ \{0\} & \text{if } k \text{ is even,} \end{cases} \tag{21}$$

where $\hat{\mathbf{Z}}$ is the profinite completion of $\mathbf{Z}$. Moreover, all of these maps induce zero on homology, and for odd k the subgroup of maps of **MU**-module spectra is given by

$$\mathbf{MU}_{k-1}\bigotimes_\mathbf{Z}(\hat{\mathbf{Z}}/\mathbf{Z}), \tag{22}$$

embedded into (21) by the coidentity on $\mathbf{MU}_*\mathbf{MU}$. It follows that for $R_* = \mathbf{MU}_* \oplus \mathbf{MU}_*\bigotimes_\mathbf{Z}\mathbf{Q}[k]$ with positive odd k, equipped with the structure of a $\mathbf{MU}_*$-algebra such that the product of two odd elements is zero, $\mathbf{E}_{R_*}$ has automorphisms which induce the identity on homology. Since (21) is bigger then (22), it even such automorphisms which also violate the structure of a **MU**-module spectrum. This means that $\mathbf{E}_{R_*}$ is not defined uniquely up to unique isomorphism by (7), that it has more than one structures of a **MU**-module spectrum, and that the first transformation in (20) does not characterise the structure of a ring spectrum on $\mathbf{E}_{R_*}$ uniquely.

In the case elliptic cohomology, these arcane perversities do not arise because we work with rings which are concentrated in even dimension. Therefore, the result of this section completes the proof of theorem 1.

4 Other families of elliptic curves

Let us explain to which families of elliptic curves the Landweber exact functor theorem can be applied. To get a formal group law, we need a commutative Noetherian ring R with unit and a flat commutative group scheme[2]

$$p\colon \mathcal{E} \to \mathrm{Spec}\, R$$

of finite type and relative dimension one, whose fibres are elliptic curves, tori or additive groups. To get a formal group law, we need a function X on some neighbourhood of the zero section of $\mathcal{E}$ which is a formal parameter of $\mathcal{E}/\mathrm{Spec}\, R$ near the zero section.

We also need a grading, thus we assume that R has a grading in even dimensions

$$R = \bigoplus_{k=-\infty}^{\infty} R_{2k}.$$

The grading defines an action of the multiplicative group $\mathcal{G}_m$ on $\mathrm{Spec}\, R$:

$$\mu_R\colon \mathcal{G}_m \times_{\mathrm{Spec}\,\mathbf{Z}} \mathrm{Spec}\, R \to \mathrm{Spec}\, R.$$

To get a formal group which is compatible with the grading, we need an action

$$\mu_{\mathcal{E}}\colon \mathcal{G}_m \times_{\mathrm{Spec}\,\mathbf{Z}} \mathcal{E} \to \mathcal{R}$$

which is compatible with the grading of R, i.e. $p\mu_{\mathcal{E}} = \mu_R p$, and with X, i.e. $\mu_{\mathcal{E}}(\lambda)^* X = \lambda X$ for any unit λ in some localisation of R_0. By the last compatibility, $\mu_{\mathcal{E}}$ is determined uniquely by X and by the grading of R, if it exists.

Let $\mathfrak{E}$ be the set of triples $(R_*, \mathcal{E}, X)$ consisting of a graded ring R_*, a group scheme $\mathcal{E}$ and a formal parameter X satisfying the conditions of the last two paragraphs. Then X and the addition in $\mathcal{E}$ define a formal group law over R_*, hence we have a homomorphism $\mathbf{MU}_* \to R_*$ respecting the grading. The Landweber conditions have the following reformulation in terms of R_* and the group scheme $\mathcal{E}$:

[2]Actually, it is not necessary to have an elliptic curve on R itself. It is sufficient if $\mathrm{Spec}R$ is the coarse moduli space for an algebraic stack of elliptic curves on which a formal parameter is given functorially. Since there do not seem to be elliptic genera in the literature which force us to consider this situation, we do not want to introduce this additional difficulty.

A The additive group of R_* has no torsion. In other words, there is no irreducible component of $\mathrm{Spec}R_*$ which is concentrated in positive characteristic.

Obviously, this corresponds to the condition that no prime number is a zero divisor in R_*.

B In characteristic $p > 0$, there are no points x of $\mathrm{Spec}R$ for which the fibre of $\mathcal{E}$ at x is an additive group.

Indeed, by theorem 3 the set of such points x is the set defined by the vanishing of (p, u_1, u_2), and also by the vanishing of $(p, u_1, \ldots, u_k)$ for any $k \leq 2$, since the additive group has height infinity. Therefore, condition **B** is implied by the condition that u_3 is no zero divisor modulo (p, u_1, u_2), and implies that u_2 is invertible modulo (p, u_1).

C For any prime number p, there is no irreducible component X of the fibre at p $\mathrm{Spec}R_* \otimes \mathbf{F}_p$ such that for any $x \in X$ the fibre $\mathcal{E}_x$ is supersingular.

Indeed, by the definition of supersingularity and by condition **B**, this is an equivalent reformulation of the assumption that u_1 is no zero divisor in $R/(p)$.

Now the Landweber exact functor theorem tells us that for any triple $\mathfrak{r} = (R_*, \mathcal{E}, X) \in \mathfrak{E}$ which satisfies the conditions **A**-**C** above, the functor

$$\mathbf{Ell}^{\mathfrak{r}}_* X = R_* \bigotimes_{\mathbf{MU}_*} \mathbf{MU}_* X$$

is a generalised homology theory. At least if R_* is countable, it is unique up to unique isomorphism in the stable homotopy category and carries a structure of a $\mathbf{MU}_*$-algebra spectrum.

One can use this to construct elliptic cohomology theories in abundance. This rises the problem to find those which are "natural" in the sense that they are related to "natural" geometric questions, like the usual elliptic theory obtained from the Jacobi quartic. While the conditions only depend on the family of elliptic curves, the problem of getting genera with good geometrical properties does not only depend on the choice of the family of elliptic curve, but also on the clever choice of a formal parameter.

For the case of the moduli problem of elliptic curves with a point of order N and an invariant form, a choice of the formal parameter X which yields good geometrical properties has been made by F. Hirzebruch [Hir88]. The task of the remaining part of this section is to show that this choice gives rise to complex oriented cohomology theories after inverting N.

Recall from [DR73, II.1] the notion of a generalised elliptic curve, which is a flat morphism $f: \mathcal{C} \to X$ of relative dimension one such that the regular set $\mathcal{C}^{\mathrm{reg}}$ has the structure of a group scheme acting on $\mathcal{C}$ and such that the geometric fibres are usual elliptic curves or Néron n-gones. Let $\tilde{\mathcal{X}}_N$ be the moduli problem which to a scheme S over $\mathrm{Spec}\mathbf{Z}[\frac{1}{N}]$ associates the set of isomorphism classes $\{\mathcal{C}, P, \omega\}$, where

- $\mathcal{C}$ is a generalised elliptic curve over S.
- $P: S \to \mathcal{C}^{\mathrm{reg}}$ is a point of precise order N such that for any geometric point $s \to S$ the image of P in $\pi_0(\mathcal{C}_s^{\mathrm{reg}})$ generates that group.
- $\omega \neq 0$ is an invariant form on $\mathcal{C}^{\mathrm{reg}}$.

Proposition 1 *Let $N \leq 2$. The moduli problem $\tilde{\mathcal{X}}_N$ is representable by a smooth scheme $\tilde{X}_N$ of relative dimension two over $\mathrm{Spec}\mathbf{Z}[\frac{1}{N}]$. Rescaling of the invariant form ω defines an action of $\mathcal{G}_{\mathrm{m}}$ on $\tilde{X}_N$. Let us call a cusp a connected component of the closed subscheme of $\tilde{X}_N$ which parametrises singular elliptic curves. Then the complement of any non-empty set of cusps in $\tilde{X}_N$ is an affine dense open subscheme.*

Proof: Let $\mathcal{X}_N$ be defined in a similar way as $\tilde{\mathcal{X}}_N$, but without the invariant form ω. Then $\tilde{\mathcal{X}}_N$ is a smooth stack over $\mathcal{X}_N$. The smoothness and algebraicity of $\mathcal{X}_N$ has been proved in [DR73, Construction IV.4.14]. It follows that $\tilde{\mathcal{X}}_N$ is algebraic and smooth of dimension two over $\mathrm{Spec}\mathbf{Z}$. Let us prove its rigidity.

Let k be an algebraically closed field of characteristic p not dividing N, and let φ be an automorphism of an elliptic curve $\mathcal{E}$ over k which fixes a point of order N and induces the identity on the tangent space at the origin. If $p = 0$, then $\varphi - \mathrm{Id}$ is either zero or etale. Since it induces zero on the tangent space, it must be zero. If $p > 0$, then $\deg \varphi - \mathrm{Id}$ must be divisible by N since a point of order N is fixed and by p since $\varphi - \mathrm{Id}$ is not etale, hence it is divisible by Np. Using the fact that $Np > 4$ one argues as in the proof of [KM85, Corollary 2.7.3] to prove $\varphi = \mathrm{Id}$. Now let $\mathcal{C}$ be a generalised elliptic curve over k, and let P be a point of order N generating the group of connected components of $\mathcal{C}^{\mathrm{reg}}$. By [DR73, II.1.10], the automorphisms of $\mathcal{C}$ are given by

$$\varphi(x) = \mu(x) \pm x,$$

where $\mu: \pi_0(\mathcal{C}^{\mathrm{reg}}) \to \mathcal{C}^{\mathrm{reg},o}$ is a group homomorphism from the group of connected components of $\mathcal{C}^{\mathrm{reg}}$ to the connected component of $\mathcal{C}^{\mathrm{reg}}$. One sees easily that P can be fixed by $\varphi \neq \mathrm{Id}$ only if one of the following cases occurs:

- $N = 2$, $\varphi(x) = -x$
- $N = 4$, $\pi_0(\mathcal{C}^{\mathrm{reg}}) = \mathbf{Z}/2\mathbf{Z}$, $\varphi(x) = \mu(x) - x$, where $\mu: \pi_0(\mathcal{C}^{\mathrm{reg}}) \to \mathcal{C}^{\mathrm{reg},o}$ is the unique non-trivial group homomorphism.

In both cases, one sees that φ cannot fix an invariant form ω.

Therefore, we know that $\tilde{\mathcal{X}}_N$ is representable by a smooth algebraic space $\tilde{X}_N$. Clearly, the action of $\mathcal{G}_{\mathrm{m}}$ on $\tilde{\mathcal{X}}_N$ by rescaling ω defines an action on $\tilde{X}_N$. To prove that $\tilde{X}_N$ is a scheme, it suffices to prove that the complement of a cusp is affine, since there are always the two disjoint cusps $\pi_0(\mathcal{C}^{\mathrm{reg}}) = \{0\}$ and $\pi_0(\mathcal{C}^{\mathrm{reg}}) = \mathbf{Z}/N\mathbf{Z}$. If $N > 4$, then [KM85, Corollary2.7.3] together with

the above consideration in the case of singular elliptic curve proves that the moduli problem $\mathcal{X}_N$ for points of order N is rigid, hence representable by a projective curve X_N by [DR73, Construction IV.4.14] and the method of the projectivity proof in [DR73, Corollaire IV.2.9]. But then the complement of any cusp in X_N is affine. Since $\tilde{X}_N$ is the space of non-zero invariant forms on the universal curve over X_N, this proves our claim if $N > 4$. If $N \leq 4$, we have to proceed in a different way. For a prime number p not dividing N, one first uses [DR73, Théorème IV.6.7] to represent the moduli problem of generalised elliptic curves with a level p structure and a point of order N by a projective curve over $\mathrm{Spec}\mathbf{Z}[\frac{1}{Np}]$. By the method used in the case $N > 4$, this implies the claim of our theorem with $\tilde{X}_N$ replaced by the moduli problem of generalised elliptic curves with a level p structure, a point of order N, and an invariant form. Using the map "forgetting the level p structure and contraction [DR73, Proposition IV.1.3]", one represents $\tilde{X}_N$ as the quotient of this moduli problem by $GL_2[\mathbf{Z}/p\mathbf{Z}]$. This proves our claim if p is inverted. Since this holds for any p, the theorem follows. **Q.E.D.**

Let $\mathcal{C}_{(N)}$ be the universal generalised elliptic curve over $\tilde{X}_N$ and let $\tilde{\mathcal{C}}_{(N)}$ be the quotient of $\mathcal{C}_{(N)}^{\mathrm{reg}}$ by its cyclic subgroup generated by P, and let $\tilde{\mathcal{C}}_{(N),o}$ be the restriction of $\tilde{\mathcal{C}}_{(N)}$ to the open subscheme $\tilde{X}_{N,o}$ parametrising non-degenerate elliptic curves. The image of the group of N-torsion points on $\mathcal{C}_{(N)}$ in $\tilde{\mathcal{C}}_{(N)}$ defines a discrete cyclic subgroup of order N $G \subset \tilde{\mathcal{C}}_{(N)}(\tilde{X}_{N,o})$. The image of $N^{-1}P$ in $\tilde{\mathcal{C}}_{(N)}$ defines a coset $M \subset \tilde{\mathcal{C}}_{(N)}(\tilde{X}_{N,o})$. Hirzebruch's choice of the formal parameter is given by

$$\begin{aligned} \mathrm{div}X &= (G) - (M) \\ d_0X &= \omega, \end{aligned} \tag{23}$$

where ω is the invariant form belonging to the moduli problem $\tilde{\mathcal{X}}_N$.

Theorem 6 *The condition (23) uniquely defines a formal parameter on $\tilde{\mathcal{C}}_{(N)}$, hence a formal group law and a homomorphism*

$$\mathbf{MU}_* \to H^0(\tilde{X}_N, \mathcal{O}_{\tilde{X}_N}). \tag{24}$$

If $U \subset \tilde{X}_N$ is a $\mathcal{G}_{\mathrm{m}}$-invariant affine open subset, then

$$\mathbf{Ell}_{N,U*}X = H^0(U, \mathcal{O}_{\tilde{X}_N}) \bigotimes_{\mathbf{MU}_*} \mathbf{MU}_*X$$

defines a **MU**-*algebra spectrum* $\mathbf{Ell}_{N,U}$ *uniquely up to unique isomorphism in the stable homotopy category. If the complement of U contains at least one cusp, then* $\mathbf{Ell}_{N,U}$ *is periodic in a non-unique way.*

Proof: By the description of the Picard group of an elliptic curve, (23) defines X as a unique formal parameter on the complement of the cusps, which is a rational

function on $\tilde{C}_{(N)}$. We have to show that the zero section is the only component of the divisor of X which meets the zero section. By the normalisation (23), it suffices to show that for any point $s \in \tilde{X}_N$ the preimage G_s of the Zariski closure of G in the fibre $\tilde{C}_{(N),s}$ at s is multiplicity free and disjoint to the preimage M_s of the Zariski closure of M. It suffices to do this when s parametrises a degenerate elliptic curve. Since the map $C^{\mathrm{reg}}_{(N)} \to \tilde{C}_{(N)}$ is finite and hence proper, G_s is the image in $\tilde{C}_{(N),s}$ of the group of N-torsion points on $C^{\mathrm{reg}}_{(N),s}$. This is a discrete cyclic subgroup of order equal to the cardinality of $\pi_0\big(C^{\mathrm{reg}}_{(N),s}\big)$. Moreover, M_s is the image of $N^{-1}P$ in $\tilde{C}_{(N),s}$ and is clearly disjoint from G_s.

This proves our claim about the existence (24). If U is a $\mathcal{G}_{\mathrm{m}}$-invariant affine open subset of $\tilde{X}_N$, we have to verify the conditions **A**–**C**. for $\tilde{C}_{(N)}$ over $H^0\big(U, \mathcal{O}_{\tilde{X}_N}\big)$. As for **A.**, this is a consequence of smoothness, **B.** follows from the very definition of the moduli problem, and **C.** follows from the fact that ordinary elliptic curves form a open dense subset in the fibre of $\tilde{X}_N$ at p.

It remains to prove the periodicity claims. If U is the complement of the cusps, then the discriminant of ω defines an invertible function on U which is homogeneous of order 12 for the $\mathcal{G}_{\mathrm{m}}$-action, hence a periodicity of order 24 for $\mathbf{Ell}_{N,U}$. By a theorem of Manin and Drinfeld [Elk90], the difference of two cusps in torsion in the Jacobian of an elliptic modular curve, hence some sort of periodicity still exists even when only one cusp is removed. **Q.E.D.**

When $N = 2$, one recovers theorem 1 from the above theorem. The necessity of inverting a homogeneous polynomial of positive degree in theorem 1 corresponds to the necessity of passing to a $\mathcal{G}_{\mathrm{m}}$-invariant open subset U in the above theorem. More precisely, $\mathbf{Ell}_P$ in theorem 1 is $\mathbf{Ell}_{2,U}$ above, where U is the complement of the set of zeros of P.

There are at least two other sorts of elliptic genera in the literature. Baker [Bak90] considers a family of Weierstraß cubics solving the moduli problem of elliptic curves with a non-zero invariant form Ω in characteristic prime to 6. He also verifies the Landweber conditions in this situation. R. Jung [Jun89] and G. Höhn [Höh91] consider a "universal elliptic genus" which links the Hirzebruch's elliptic genera for varying N. The conditions **A.**–**B.** for this family of elliptic curves should be accessible to direct calculations. One could perhaps try to use this to replace the abstract moduli theory which we used in our approach to $\mathbf{Ell}_{N,U}$ by explicit calculations. We leave all this to the reader.

5 A proof of the Chudnovsky-Landweber congruences

Landweber based is verification of condition 3 on page 5 on the congruences

$$u_2 \equiv \left(\frac{-1}{p}\right)\varepsilon^{\frac{p^2-1}{4}} \pmod{(p, u_1)}$$

$$(\delta^2-\varepsilon)^{\frac{p^2-1}{4}} \equiv \varepsilon^{\frac{p^2-1}{4}} \pmod{(p,u_1)}.$$

As we have seen in the last two sections, this is not necessary. Nevertheless, it may still be interesting to prove the congruences. The original proof of Chudnovsky is based on the Atkin-Swinnerton-Dyer congruences. Two proofs in [Lan88c] were based on a calculation of B. Gross for Weierstraß cubics and on formulas of Igusa for multiplication by n in the Jacobia quartic. We follow Gross' ideas, but work directly with the Jacobi quartic. This allows us to avoid much of the computational labour in [Lan88c], without seriously complicating the theoretical background on which the proof depends.

Let $\mathcal{E}$ be an elliptic curve over a field k of characteristic $\neq 2$, let $P \in \mathcal{E}_2 - \{0\}$ be a point of exact order 2 on $\mathcal{E}$, and let ω be a non-vanishing invariant form on $\mathcal{E}$. As we shall see below, the triple $(\mathcal{E}, P, \omega)$ has a unique realisation as a Jacobi quartic. We will also consider the factor curve $\tilde{\mathcal{E}} = \mathcal{E}/\{0, P\}$ (cf. [Mum88, §II.7.] for a description of the quotient of an algebraic manifold by a finite group). Let $\pi: \mathcal{E} \to \tilde{\mathcal{E}}$ be the projection. Then

$$\tilde{P} = \pi(\mathcal{E}_2 - \{0, P\})$$

is a point of precise order 2 on $\tilde{\mathcal{E}}$. There is a unique invariant form $\tilde{\omega}$ on $\tilde{\mathcal{E}}$ with $\pi^*\tilde{\omega} = \omega$. Let us first derive the equation of the Jacobi quartic, and some other useful formulas. They are well-known from the theory of elliptic and modular functions of one variable, cf. [Igu59].

Proposition 2 *1. There is a unique rational function X on $\mathcal{E}$ with*

$$\mathrm{div} X = (0) + (P) - (\mathcal{E}_2 - \{0, P\})$$

and

$$d_0 X = \omega(0).$$

It satisfies the relations

$$\begin{aligned} X(a+P) &= -X(a) \\ X(-a) &= -X(a). \end{aligned} \tag{25}$$

2. There is a unique rational function Y on $\mathcal{E}$ with

$$\mathrm{div} Y = \sum_{\substack{Q \in \mathcal{E}_4 \\ 2Q = P}} (Q) - 2(\mathcal{E}_2 - \{0, P\})$$

and $Y(0) = 1$. It satisfies the relations

$$\begin{aligned} Y(a+P) &= -Y(a) \\ Y(-a) &= Y(a). \end{aligned} \tag{26}$$

3. *There unique constants δ, $\varepsilon \in k$ such that*

$$Y^2 = 1 - 2\delta X^2 + \varepsilon X^4, \tag{27}$$

and the map $P \to (X(P), Y(P))$ defines an isomorphism of $\mathcal{E} - (\mathcal{E}_2 - \{0, P\})$ with the affine curve (27).

4. *The invariant form is given by*

$$\omega = \frac{dX}{Y}. \tag{28}$$

5. *Let $\tilde{X}$ and $\tilde{Y}$ on $\tilde{\mathcal{E}}$ be defined in the same way as X and Y, using $\tilde{P}$ and $\tilde{\omega}$. Then the pull-backs of $\tilde{X}$ and $\tilde{Y}$ to $\mathcal{E}$ are given by*

$$\begin{aligned} \pi^* \tilde{X} &= \frac{X}{Y} \\ \pi^* \tilde{Y} &= \frac{1 - \varepsilon X^4}{Y^2} = \frac{1 - \varepsilon X^4}{(1 - 2\delta X^2 + \varepsilon X^4)^2}. \end{aligned} \tag{29}$$

6. *The constants δ and ε for the triple $(\tilde{\mathcal{E}}, \tilde{P}, \tilde{\omega})$ are $\tilde{\delta} = -2\delta$ and $\tilde{\varepsilon} = 4(\delta^2 - \varepsilon)$.*

Proof: The existence and uniqueness of X and Y follow from the well-known description of the divisor class groups of elliptic curves. Since $-X(-a)$ and $Y(-a)$ satisfy the conditions which characterise X and Y uniquely, the second formulas in (25) and (26) follow. For the same reason, the first of the formulas in (25) and (26) have to be true up to a sign, and to complete their proof we only have to exclude the possibility that $X(a + P) = X(a)$ or $Y(a + P) = Y(a)$. If the first of these relations was true, then X would come from a rational function f on $\tilde{\mathcal{E}}$ with $\operatorname{div} f = (0) - \tilde{P}$. By the description of the divisor class group of $\tilde{\mathcal{E}}$, no such function f exists. If we had $Y(a + P) = Y(a)$, then $Y = \pi^* g$, where $\operatorname{div} g = 2(\tilde{P}) - (\tilde{\mathcal{E}} - \{0, \tilde{P}\})$, which is impossible.

To get the equation for the Jacobi quartic, we represent $\tilde{\mathcal{E}}$ as a ramified double cover $p: \tilde{\mathcal{E}} \to \mathbf{P}^1$ with $p(-a) = p(a)$ and $p(\tilde{P}) = \infty$. Then all the summands in the equation (27) are functions f on $\mathcal{E}$ with $f(a + P) = f(-a) = f(a)$ and with poles of order ≤ 4 in $\mathcal{E}_2 - \{0, P\}$ and no other pole. A function f with these properties has the form $\pi^* p^* g$, where g is a polynomial of degree ≤ 2. Since there are only three such polynomials but four summands in (27), a relation of type (27) must hold, by the normalisation for Y.

To verify that $\mathcal{E} - (\mathcal{E}_2 - \{0, P\})$ is mapped isomorphically to the Jacobi quartic, let a and $\tilde{a}$ have the same finite coordinates X and Y. By the symmetry properties, $X(a) = X(P - a)$. By the description of the divisor of X, X is of degree two, hence we must have $\tilde{a} = P - a$. But $Y(P - a) = -Y(a)$, hence $Y(a) = 0$ since p is odd, hence $2a = P$, hence $\tilde{a} = P - a = a$. This shows that the map from $\mathcal{E} - (\mathcal{E}_2 - \{0, P\})$ to the Jacobi quartic is one-to one. One verifies that its differential is not zero, for instance by the formula for the invariant differential ω.

Since the right hand side of (28) has the correct value at 0, to verify (28) it suffices to prove that its right hand side has no poles, because then it must be a multiple of ω. The possible candidates for poles of the right hand side of (28) are the second order poles of dX and the first order zeros of Y. But the poles of dX are cancelled by the poles of Y, and by (27) the zeros of Y are also zeros of dX.

The first of the formulas (29) holds because its right hand side has the correct divisor and the correct differential at 0. To verify the formula for $\pi^*\tilde{Y}$, note that $\pi^*\tilde{Y}$ is uniquely determined by $\omega = \frac{d\pi^*\tilde{X}}{\pi^*\tilde{Y}}$. But

$$\begin{aligned}
\frac{d\pi^*\tilde{X}}{\frac{1-\varepsilon X^4}{Y^2}} &= \frac{\frac{Y\,dX - X\,dY}{Y^2}}{\frac{1-\varepsilon X^4}{Y^2}} \\
&= \frac{Y^2\,dX - \frac{1}{2}X\,dY^2}{Y(1-\varepsilon X^4)} \\
&= \frac{1 - 2\delta X^2 + \varepsilon X^4 + 2\delta X^2 - 2\varepsilon X^4}{1-\varepsilon X^4}\frac{dX}{Y} \\
&= \omega.
\end{aligned}$$

Finally, we have

$$\begin{aligned}
\pi^*\tilde{Y}^2 &= \frac{(1-\varepsilon X^4)^2}{Y^4} \\
&= \frac{1 - 2\varepsilon X^4 + \varepsilon^2 X^8}{Y^4} \\
&= \frac{(1 - 2\delta X^2 + \varepsilon X^4)^2 + 4\delta X^2(1 - 2\delta X^2 + \varepsilon X^4) + 4(\delta^2 - \varepsilon)X^4}{Y^4} \\
&= 1 + 4\delta\pi^*\tilde{X}^2 + 4(\delta^2 - \varepsilon)\pi^*\tilde{X}^4,
\end{aligned}$$

proving our formulas for $\tilde{\delta}$ and $\tilde{\varepsilon}$. **Q.E.D.**

We are now ready to prove the main result of this talk.

Theorem 7 *Let $\mathcal{E}$ be a supersingular elliptic curve over a field k of characteristic $p > 2$, and let $P \in \mathcal{E}(k)$ be a point of precise order 2. Let ω be a invariant differential form on $\mathcal{E}$, and let X, δ, ε be defined in the same way as in the above proposition. Then*

$$[p]^*X = u_2 X^{p^2} \tag{30}$$

with

$$u_2 = \varepsilon^{\frac{p^2-1}{4}}\left(\frac{-1}{p}\right). \tag{31}$$

Furthermore,

$$(\varepsilon^2 - \delta)^{\frac{p^2-1}{4}} = \varepsilon^{\frac{p^2-1}{4}}. \tag{32}$$

Proof: We follow B. Gross' arguments for the Weierstrass cubic, which were explained in [Lan88c]. It is clear that the validity of our formulas does not depend on the choice of ω. Since it is known (or will follow from considerations below) that there are only finitely many isomorphism classes of supersingular curves, we may assume $k = \overline{\mathbf{F}}_p$. We will choose an appropriate model for $\mathcal{E}$ over $\mathbf{F}_{p^2}$. Then our formulas will turn out to be essentially rationality assertions. The arguments in the next paragraph give a refined version of the classical fact that any supersingular elliptic curve lives over $\mathbf{F}_{p^2}$. We will use the standard facts about descending elliptic curves over algebraically closed fields to smaller subfields, as explained, for instance, in [Hus87, Chapter 7].

Let $\mathrm{Frob}_p: \mathcal{E} \to \mathcal{E}^{(p)}$ be the Frobenius and let $V_p: \mathcal{E}^{(p)} \to \mathcal{E}$ be the Verschiebung, the dual of Frob_p. While Frob_p is always purely inseparable, V_p is purely inseparable if and only if $\mathcal{E}$ is supersingular. Recall that two purely inseparable covers of a curve over a perfect field are isomorphic, cf. [Sil86, Corollary II.2.12]. Applying this to the inseparable covers $\mathcal{E}$ (via Frob_p) and $\mathcal{E}^{(p^2)}$ (via V_p) of $\mathcal{E}^{(p)}$, we see that there exists an isomorphism $\psi: \mathcal{E} \cong \mathcal{E}^{(p^2)}$. Applying the same fact to the two inseparable covers of degree p^2 of $\mathcal{E}$, $\mathcal{E}$ via $\psi^{-1}\mathrm{Frob}_{p^2}$ and $\mathcal{E}$ via $[p]$, we see that there exists an automorphism A of the curve $\mathcal{E}$ such that $\psi^{-1}\mathrm{Frob}_{p^2} = A[p]$. At the price of changing ψ, we may achieve that $A = [\left(\frac{-1}{p}\right)]$. Let $\mathbf{E}$ be the model of $\mathcal{E}$ over $\mathbf{F}_{p^2}$ obtained by descent with respect to ψ. Then the relative Frobenius is

$$\mathrm{Frob}_{\mathbf{E}/\mathbf{F}_{p^2}} = [\left(\frac{-1}{p}\right)p]. \tag{33}$$

This relative Frobenius is characterised by the property that pull-back by it maps any $\mathbf{F}_{p^2}$-rational function to its p^2-the power. The $\mathbf{F}_{p^2}$-model $\mathbf{E}$ is defined in such a way that $\mathrm{Frob}_{\mathbf{E}/\mathbf{F}_{p^2}} = \psi^{-1}\mathrm{Frob}_{p^2}$, whence (33). The crucial observation which brings the Jacobi symbol into the play is that this endomorphism of $\mathcal{E}$ acts as multiplication by $\left(\frac{-1}{p}\right)p \equiv 1$ on points of order 4, hence the model $\mathbf{E}$ has all its points of order 4 defined over $\mathbf{F}_{p^2}$.[3]

As was indicated above, the matter is independent of ω, hence we may assume that ω and X and Y are defined for the model $\mathbf{E}$. Then $\mathrm{Frob}_{\mathbf{E}/\mathbf{F}_{p^2}}{}^* X = X^{p^2}$, hence (33) implies (30) with $u_2 = \left(\frac{-1}{p}\right)$. To prove (31) we have to show $\varepsilon^{\frac{p^2-1}{4}} = 1$, i.e., that ε is a fourth power in $\mathbf{F}_{p^2}$. Recall the factor curve $\tilde{\mathcal{E}} = \mathcal{E}/\{0, P\}$. It is also defined over $\mathbf{F}_{p^2}$, as are $\tilde{X}$ and $\tilde{Y}$. Let $Q \in \mathbf{E}_4$ such that $2Q \notin \{0, P\}$. By the definition of $\tilde{Y}$, πQ is a zero of $\tilde{Y}$, hence $\varepsilon X(Q)^4 = 1$ by (29). This proves that ε is a fourth power in $\mathbf{F}_{p^2}$ and completes our proof of (30) and of (31).

[3] The possibility of replacing A by $-A$ corresponds precisely to the twist considered at the end of [Lan88c, p. 80]. However, the separate treatment of the cases $j \in \{0; 1728\}$ is not necessary since in these cases we also have more automorphisms to twist with.

We have already seen that ε is a fourth power in $\mathbf{F}_{p^2}$, hence the right hand side of (32) is equal to one. On the other side, the condition (33) is invariant under isogenies, it is also satisfied by $\tilde{\mathbf{E}} = \mathbf{E}/\{0, P\}$. Since $\tilde{\omega}$ is clearly $\mathbf{F}_{p^2}$-rational, $\tilde{\varepsilon} = 4(\delta^2 - \varepsilon)$ is also a fourth power in $\mathbf{F}_{p^2}$. Since $4^{\frac{p^2-1}{4}} \equiv 1 \pmod{p}$, this means that the left hand side of (32) is also equal to one. **Q.E.D.**

Now we consider the general Jacobi quartic

$$y^2 = 1 - 2\delta x^2 + \varepsilon x^4.$$

Up to a double point at infinity, this is a semielliptic curve over $\mathrm{Spec}\mathbf{Z}[\frac{1}{2}, \delta, \varepsilon] - \{(0,0)\}$ with multiplicative reduction along the cusps $\varepsilon = 0$ (connected Néron model) and $\delta^2 - \varepsilon = 0$ (Néron model has two components). The identity is the point $(0, 1)$. For an odd prime number p, consider the power series

$$[p]^* x = px + \ldots + u_1 x^p + \ldots + u_2 x^{p^2}.$$

It is well known that the relation $p = u_1 = 0$ characterises supersingular elliptic curves. The result of our theorem can therefore be reformulated as

$$\begin{aligned} u_2 &\equiv \left(\frac{-1}{p}\right) \varepsilon^{\frac{p^2-1}{4}} \pmod{\mathrm{rad}(p, u_1)} \\ (\delta^2 - \varepsilon)^{\frac{p^2-1}{4}} &\equiv \varepsilon^{\frac{p^2-1}{4}} \pmod{\mathrm{rad}(p, u_1)}. \end{aligned}$$

Our task was to prove these congruences modulo the ideal (p, u_1) itself. It suffices to show that this ideal is the intersection of maximal ideals. Here we simply reproduce Igusa's well known argument (applied to Legendre polynomials instead of the Deuring polynomials), as in [Lan88c].

Proposition 3 *We have*

$$\mathrm{rad}(p, u_1) = (p, u_1).$$

Proof: Let $F(x, \tilde{x})$ be the formal group law and let

$$\omega = \sum_{k=0}^{\infty} \omega_k(\delta, \varepsilon) x^k, \qquad \omega_0 = 1,$$

be the invariant differential for the universal Jacobi quartic. We first want to verify

$$u_1 \equiv \omega_{p-1} \pmod{p}. \tag{34}$$

To this end, note that

$$\log(x) = \sum_{k=1}^{\infty} \frac{\omega_{k-1}(\delta, \varepsilon)}{k} x^k \in \mathbf{Q}[\delta, \varepsilon][[x]]$$

is the logarithm of the formal group law, satisfying $\log(F(x,\tilde{x})) = \log(x) + \log(\tilde{x})$, and let

$$\exp(x) = \sum_{k=1}^{\infty} e_k(\delta,\varepsilon)x^k, \qquad c_1 = 1,$$

be the inverse of log. Then for $1 \leq k \leq p-1$, $\frac{\omega_{k-1}}{k}$ is a polynomial in δ and ε with p-integral coefficients, consequently the polynomials $e_k(\delta,\varepsilon)$ also have p-integral coefficients if $1 \leq k \leq p-1$. Also, pe_p is p-integral. It follows that

$$[p]x = \exp(p\log(x)) \equiv \omega_{p-1}x^p \pmod{(x^{p+1},p)},$$

which was to be proved.

Now recall the Legendre polynomials $P_k(\xi)$, which are defined by

$$\frac{1}{\sqrt{1-2x\xi+x^2}} = \sum_{k=1}^{\infty} P_k(\xi)x^k.$$

By (34) and our formula for the invariant differential on a Jacobi quartic, this implies

$$u_1(\delta,\varepsilon) \equiv P_{\frac{p-1}{2}}(\frac{\delta}{\sqrt{\varepsilon}})\varepsilon^{\frac{p-1}{2}} \pmod{p}.$$

Consequently, it suffices to show that $P_{\frac{p-1}{2}}$ has no double zeros modulo p.

Note that the Legendre polynomials satisfy the differential equation

$$(1-x^2)P_n''(x) - 2xP_n'(x) + n(n+1)P_n(x) = 0. \tag{35}$$

Since $P_n(\pm 1) = (\pm 1)^n$, ± 1 are not zeros of P_n modulo p. If $x \notin \{\pm 1\}$ is a double zero of P_n modulo p, then it follows by induction from (35) that all derivatives of P_n vanish modulo p at x. If $n := \deg P_n < p$, this would imply P_n vanish modulo p, which we know it does not. This proves that $P_{\frac{p-1}{2}}$ has no double zeros modulo p, and completes our lecture. **Q.E.D.**

References

[Ada74] J. F. Adams. *Stable Homotopy and Generalised Homology*, volume 10 of *Chicago Lectures in Mathematics*. The University of Chicago Press, 1974.

[Bak90] Andrew Baker. Hecke operators as operations in elliptic cohomology. *Journal of Pure and Applied Algebra*, 63:1–11, 1990.

[DR73] P. Deligne and M. Rapoport. Les schémes de modules des courbes elliptiques. In *Modular Functions of One Variable II*, volume 349 of *Lecture Notes in Mathematics*, pages 143–316, 1973.

[Elk90] R. Elkik. Le théorème de Manin-Drinfeld. In Lucien Szpiro, editor, *Séminaire sur les Piceaux de Courbes elliptiques (a la recherche de "Mordell effiectif")*, volume 183 of *Astérisque*, 1990.

[Hir88] Friedrich Hirzebruch. Elliptic genera of level N for complex manifolds. In K. Bleuler and M. Werner, editors, *Differential Geometric Methods in Theoretical Physics*, pages 37–63, 1988.

[Höh91] G. Höhn. Diplomarbeit, Bonn. 1991.

[Hus87] Dale Husemoller. *Elliptic Curves*, volume 111 of *Graduate Texts in Mathematics*. Springer, 1987.

[Igu59] Jun-ichi Igusa. On the transformation theory of elliptic functions. *American Journal of Mathematics*, 81:436–452, 1959.

[Jun89] R. Jung. Diplomarbeit, Bonn. 1989.

[KM85] Nicholas M. Katz and Barry Mazur. *Arithmetic Moduli of Elliptic Curves*, volume 108 of *Annals of Mathematics Studies*. Princeton University Press, 1985.

[KS91] Matthias Kreck and Stefan Stolz. HP^2-bundles and elliptic homology. Preprint, MPI/91-46, 1991.

[Lan76] Peter S. Landweber. Homological properties of comodules over $MU_*(MU)$ and $BP_*(BP)$. *American Journal of Mathematics*, 98(3):591–617, 1976.

[Lan88a] Peter S. Landweber. Elliptic cohomology and modular forms. In *Elliptic Curves and Modular Forms in Algebraic Topology* [Lan88b], pages 55–68. Proceedings, Princeton 1986.

[Lan88b] Peter S. Landweber, editor. *Elliptic Curves and Modular Forms in Algebraic Topology*, volume 1326 of *Lecture Notes in Mathematics*. Springer, 1988. Proceedings, Princeton 1986.

[Lan88c] Peter S. Landweber. Supersingular elliptic curves and congruences for Legendre polynomials. In *Elliptic Curves and Modular Forms in Algebraic Topology* [Lan88b], pages 69–93. Proceedings, Princeton 1986.

[Laz64] Daniel Lazard. Sur les modules plats. *Comptes Rendus Acad. Sc. Paris*, 258:6313–6316, June 1964. Groupe 1.

[LRS] Peter S. Landweber, Douglas C. Ravenel, and Robert E. Stong. Periodic cohomology theories defined by elliptic curves. to appear.

[MR77] Haynes R. Miller and Douglas C. Ravenel. Morava stabilizer algebras and the localization of Novikov's E_2-term. *Duke Mathematical Journal*, 44(2):433–447, June 1977.

[Mum88] David Mumford. *Abelian Varietites.* Tata Institute of Fundamental Research Studies in Mathematics. Oxford University Press, 1988.

[Qui69] Daniel G. Quillen. On the formal groups laws of unoriented and complex cobordism theory. *Bulletin of the American Mathematical Society*, 75:1293–1298, 1969.

[Qui71] Daniel G. Quillen. Elementary proofs of some results of cobordism theory using Steenrod operations. *Advances in Mathematics*, 7:29–56, 1971.

[Rav84] Douglas C. Ravenel. Localization with respect to certain periodic homology theories. *American Journal of Mathematics*, 106:351–414, 1984.

[Rav86] Douglas C. Ravenel. *Complex Cobordism and Stable Homotopy Groups of Spheres*, volume 121 of *Pure and Applied Mathematics.* Academic Press, Inc., 1986.

[Seg88] Graeme Segal. Elliptic cohomology. In *Séminaire Bourbaki 1987/88*, Astérisque, pages 187–201. 1988.

[Sil86] Joseph H. Silverman. *Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics.* Springer, 1986.

[Swi75] Robert M. Switzer. *Algebraic Toplogy—Homotopy and Homology*, volume 212 of *Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen.* Springer, 1975.

[Yos88] Zen-ichi Yosimura. Hausdorff condtition for Brown-Peterson cohomologies. *Osaka Journal of Mathematics*, 25:881–890, 1988.