FORMAL GROUPS AND CONGRUENCES FOR L-FUNCTIONS

By Jan Stienstra

Introduction. In this note we show congruences, similar to those of Atkin and Swinnerton-Dyer [2, 6], for a large class of schemes, including branched double coverings of $\mathbf{P}^N$ of arbitrary dimension and genus, defined over any ring which is flat and of finite type over $\mathbf{Z}$. The results of sections 1-4 together yield the following theorem.

Theorem 0.1. *Let K be a ring which is flat and of finite type over $\mathbf{Z}$. Let $R \in K[T_0, \ldots, T_N]$ be a homogeneous polynomial of degree $2d$. Assume $2d > 2N > 0$. Let $\mathfrak{X}$ be the double covering of $\mathbf{P}^N_K$ given by the equation $U^2 = R$ (where U is a new variable of weight d).*

Let $\mathcal{P}$ be a maximal ideal of K with residue field $K/\mathcal{P}$ of characteristic p and of order $q = p^f$. Let e be an integer such that $1 \leqslant e \leqslant p - 1$ and $p \in \mathcal{P}^e$.

Let $\mathfrak{X}_{\mathcal{P}} = \mathfrak{X} \times_{\operatorname{spec} K} \operatorname{spec}(K/\mathcal{P})$ be the fibre of $\mathfrak{X}$ at $\mathcal{P}$. Assume that there exist a smooth projective variety X over $K/\mathcal{P}$ and a morphism $\pi : X \to \mathfrak{X}_{\mathcal{P}}$ such that $\pi_*\mathcal{O}_X = \mathcal{O}_{\mathfrak{X}_{\mathcal{P}}}$ and $R^i\pi_*\mathcal{O}_X = 0$ for $i \geqslant 1$. Let

$$P_N(T) = \det(1 - TF_q \,|\, H^N_{cris}(X) \otimes \mathbf{Q}),$$

the (reversed) characteristic polynomial of the Frobenius operator F_q, relative to $K/\mathcal{P}$, acting on the middle crystalline cohomology group of X; say

$$P_N(T) = a_0 + a_1T + \cdots + a_kT^k \in \mathbf{Z}[T].$$

Let $J = \{i = (i_0, \ldots, i_N) \in \mathbf{Z}^{N+1} \,|\, i_0, \ldots, i_N \geqslant 1, i_0 + \cdots + i_N = d\}$ and

$$g = \binom{d-1}{N}. \qquad \textit{So} \quad g = \#J = \dim_{K/\mathcal{P}} H^N(X, \mathcal{O}_X).$$

Manuscript received 16 March 1986.

American Journal of Mathematics 109 (1987), 1111-1127.

Define for every positive integer n a g × g — matrix β_n, with rows and columns indexed by the elements of the set J and with entries in K, by: the entry of β_n in row i and column j is

$$\beta_{n,i,j} = \textit{the coefficient of } T_0^{nj_0-i_0}\cdot \ldots \cdot T_N^{nj_N-i_N} \textit{ in } R^{(n-1)/2} \textit{ if } n \textit{ is odd,}$$

$$\beta_{n,i,j} = 0 \quad \textit{if} \quad n \textit{ is even.}$$

Consider the formal Dirichlet series

$$P_N(q^{-s}) = 1 + a_1q^{-s} + a_2q^{-2s} + \cdots + a_kq^{-ks}, \qquad \sum_{n\geqslant 1} \beta_n n^{-s}$$

and their product

$$\sum_{n\geqslant 1} \theta_n n^{-s} = \Big(\sum_{n\geqslant 1} \beta_n n^{-s}\Big)\cdot P_N(q^{-s}).$$

So $\theta_n = \beta_n + a_1\beta_{n/_q} + a_2\beta_{n/_{q^2}} + \cdots + a_k\beta_{n/_{q^k}}$, where, by convention, $\beta_u = 0$ if $u \notin \mathbf{Z}$.

Then we have for every $n \in \mathbf{N}$ the congruence relation

$$\theta_n \equiv 0 \bmod \mathcal{P}^{ev-efg+1} \quad \textit{if} \quad n \equiv 0 \bmod p^v, \qquad v \geqslant fg$$

(i.e. each entry of the matrix θ_n is in the indicated power of $\mathcal{P}$). □

Remark 0.2. If we add in (0.1) the hypothesis that for every $x \in K$ and for every integer $w > e$ one has $px \in \mathcal{P}^w$ if and only if $x \in \mathcal{P}^{w-e}$, then we can define the function $\mathrm{ord}_{\mathcal{P}} : K \otimes \mathbf{Q} \to \mathbf{Z}$ by $\mathrm{ord}_{\mathcal{P}}((x \otimes 1/n) = w - ev$ if $x \in \mathcal{P}^w \backslash \mathcal{P}^{w+1}$ and $n \in p^v\mathbf{Z}\backslash p^{v+1}\mathbf{Z}$. This function can be extended to matrices over $K \otimes \mathbf{Q}$ by $\mathrm{ord}_{\mathcal{P}}((a_{ij})_{ij}) = \min_{i,j} \mathrm{ord}_{\mathcal{P}}(a_{ij})$.

In terms of this function the congruences in (0.1) can be reformulated as

$$\mathrm{ord}_{\mathcal{P}}(\theta_n/n) \geqslant 1 - efg \quad \text{for all} \quad n \in \mathbf{N}.$$

0.3. The inverse $P_N(q^{-s})^{-1}$ of the Dirichlet series $P_N(q^{-s})$ in (0.1) is by definition the *L-function* for the middle (crystalline) cohomology of X. It would be more appealing to call it the *local L-function* of $H^N(\mathcal{X})$ at the closed point $\mathcal{P}$ of spec K, but to justify that terminology the connection between $\mathcal{X}$ and X must be made more canonical, for instance by assuming

$\mathfrak{X}_{\mathcal{P}}$ smooth and $X = \mathfrak{X}_{\mathcal{P}}$, or by a theory of smooth minimal models. On the other hand, the congruences yield only information about the roots of $P_N(T)$ of p-adic valuation $<f$ (or $>(N-1)f$, by duality), i.e. about the part of $H^N_{cris}(X) \otimes \mathbf{Q}$ where Frobenius F_p acts with slopes <1. This part is isomorphic with $H^N(X, \mathcal{W}\mathcal{O}_X) \otimes \mathbf{Q}$ and is independent of the particular choice of the desingularization $\pi : X \to \mathfrak{X}_{\mathcal{P}}$, as long as the condition for $R^{\cdot}\pi_*\mathcal{O}_X$ is satisfied (cf. 2.5, 3.1, 3.2). So maybe one should try to formulate the result for a suitable factor of $P_N(q^{-s})^{-1}$, which is independent of the choice of X and which can be considered as the local *L-function* at $\mathcal{P}$ of a sub-motive of $H^N(\mathfrak{X})$.

Examples. 0.4. (a). The original Atkin-Swinnerton-Dyer congruences [2] for an elliptic curve with equation

$$y^2 = x^3 + Ax + B, \qquad A, B \in \mathbf{Z}_p$$

are covered by theorem (0.1): One takes $N = 1$, $d = 2$ and

$$R = T_0T_1^3 + AT_0^3T_1 + BT_0^4.$$

Beukers [3] showed that the p-adic integers β_n of theorem (0.1) are in fact the coefficients of the expansion of the canonical differential form $\omega = dx/2y$ in terms of the coordinate $u = -x/y$ at infinity:

$$\omega = \frac{dx}{2y} = \sum_{n \geqslant 1} \beta_n u^{n-1} du.$$

A generalization of this connection between the β_n's and differential forms for higher dimension and genus is shown in [17].

The congruences for the elliptic curve read

$$\beta_{np} + a_1\beta_n + p\beta_{n/p} \equiv 0 \bmod p^{\nu+1} \quad \text{if} \quad p^\nu | n.$$

Note that the number of $\mathbf{F}_p$-rational points on the elliptic curve is $1 + a_1 + p$. If p is at least 17, the integer a_1 can already be computed from the single congruence $a_1 \equiv -\beta_p \bmod p$ and the archimedean estimate $|a_1| \leqslant 2\sqrt{p}$, given by the Weil conjectures (cf. [7]).

(b). In [16] we gave congruences of Atkin-Swinnerton-Dyer type for certain K3-surfaces. The examples of op. cit. are also covered by theorem (0.1). For instance, the smooth minimal model of the equation

$$U^2 = -T_0T_1T_2(T_0 + T_1)(T_1 + T_2)(T_2 + T_0)$$

in characteristics $\neq 2$ is a $K3$-surface. The integers β_n for this equation are: $\beta_n = 0$ for even n,

$$\beta_n = (-1)^m \sum_k \binom{m}{k}^3 \quad \text{if} \quad n = 2m + 1.$$

The polynomial $P_2(T)$ for the smooth minimal model of the above equation over the prime field $\mathbf{F}_p$ was also computed in [16]:

$$P_2(T) = (1 - pT)^{20}(1 + aT + \epsilon p^2T^2)$$

with $a = 0$ and $\epsilon = -1$ if $p \equiv 5$ or $7 \bmod 8$, resp. $a = 2p - 4u^2$ and $\epsilon = 1$ if $p = u^2 + 2v^2$, u, $v \in \mathbf{Z}$. For the congruences one can omit the factors $(1 - pT)$, only $1 + aT + \epsilon p^2T^2$ is relevant (cf. (0.3)). The congruences reduce to

$$\beta_{np} + a\beta_n + \epsilon p^2\beta_{n/p} \equiv 0 \bmod p^{\nu+1} \quad \text{if} \quad p^\nu | n.$$

The situation in this example is quite exceptional, in that one has an alternative way for determining $P_2(T)$. In general this polynomial will be unknown. Through the congruences one can then obtain some information about it.

(c). A prominent theme in Dwork's work is the variation of the zeta function in a family of varieties (see [22, 24] and the bibliography therein). In (0.1) that amounts to studying $P_N(T)$ as $\mathcal{P}$ varies over the closed points of spec K, with or even without fixing the residue characteristic. The internal combinatorics of the construction of the matrices β_n is probably so strong that the congruences of (0.1) "converge" to p-adic limit formulas for the roots of $P_N(T)$ of p-adic valuation less than deg $\mathcal{P} = [K/\mathcal{P} : \mathbf{F}_p]$. Moreover these limit formulas should be related to the Gauss-Manin connection ($\approx$ Picard-Fuchs equation) for $\mathfrak{X}/K/\mathbf{Z}$ (cf. [22, 24]).

0.5. This paper is organized as follows. Congruences of the kind we are looking for, are the output of a simple fairly general theorem on formal groups, treated in section 1. The input data for this theorem are a formal group G over a $\mathbf{Z}$-flat ring K, the logarithm of a curvilinear formal group law for G (characteristic 0 data) and information about the action of Frobenius on the Cartier module of curves on the reduction of G modulo an ideal of K (characteristic p data). The formal groups we use, are those of Artin and Mazur [1]; their definition is recalled in section 2. Information about the action of Frobenius in characteristic p comes via Witt vector cohomology and crystalline cohomology from the zeta function of the scheme. These matters are discussed in section 3. The characteristic 0 input data are provided by [17]. In op. cit. we construct an explicit logarithm of a curvilinear formal group law for the only interesting Artin-Mazur formal group for complete intersections, with degree restrictions, in $\mathbf{P}^M$ and for branched double coverings of $\mathbf{P}^N$. In section 4 we briefly describe the result for the double coverings. The combination of this result with the results of sections 1-3 constitutes a proof of theorem (0.1). A similar theorem can be proved for complete intersections by combining sections 1-3 with theorem 1 of [17].

0.6. For other generalizations of the original Atkin-Swinnerton-Dyer congruences see [19, 20, 21, 23, 25, 26].

1. Generalities on formal groups and congruences.

References for this section are [8, 9, 15, 18, 5]. By formal group we mean smooth commutative formal group. The rings and algebras in this paper are associative and commutative and all rings have a unit element.

1.1. Let K be a ring and let g be a positive integer. Let $\mathcal{N}\mathit{ilalgs}_K$ denote the category of *nil-K-algebras*, i.e. of K-algebras in which every element is nilpotent. *Formal affine g-space over K* is the functor $\mathbf{A}_K^g$: $\mathcal{N}\mathit{ilalgs}_K \rightarrow \mathcal{S}\mathit{ets}$ which assigns to a nil-K-algebra A the set $A \times \cdots \times A$ (g factors) and to a morphism f the map $f \times \cdots \times f$. A *g-dimensional formal group over K* is a functor $\mathcal{G} : \mathcal{N}\mathit{ilalgs}_K \rightarrow \mathcal{A}\mathit{belian\ groups}$ whose underlying set valued functor admits a functorial bijection onto $\mathbf{A}_K^g$. Such a functorial bijection $\mathcal{G} \rightarrow \mathbf{A}_K^g$ is called a *coordinatization* of the formal group $\mathcal{G}$.

1.2. A coordination $c : \mathcal{G} \rightarrow \mathbf{A}_K^g$ leads to a description of the formal group $\mathcal{G}$ by a *g-dimensional formal group law* $L(\xi, \eta)$ over K: there exists a g-tuple $L = (L_1, . ., L_g)$ of formal power series with coefficients in K in two g-tuples of variables $\xi = (\xi_1, . ., \xi_g)$ and $\eta = (\eta_1, . ., \eta_g)$ such that for every nil-K-algebra A and for all elements $\alpha, \beta \in \mathcal{G}(A)$:

$$c(\alpha \boxplus \beta) = L(c(\alpha), c(\beta));$$

here $\boxplus$ denotes the group structure on $\mathcal{G}$. The group axioms for $\mathcal{G}$ correspond to the following identities for $L(\xi, \eta)$:

$$L(L(\xi, \eta), \zeta) = L(\xi, L(\eta, \zeta)), \qquad L(\xi, 0) = \xi,$$

$$L(\xi, \eta) = L(\eta, \xi), \qquad L(\xi, \eta) \equiv \xi + \eta \bmod \deg \geqslant 2;$$

here ζ is another g-tuple of variables and $0 = (0, \ldots, 0)$.

1.3. If K is a $\mathbf{Z}$-flat ring (i.e. the canonical map $K \to K \otimes \mathbf{Q}$ is injective), every g-dimensional formal group law $L(\xi, \eta)$ over K determines a g-tuple $\ell(\tau)$ of power series in one g-tuple of variables τ with coefficients in $K \otimes \mathbf{Q}$ such that

$$\ell(\tau) \equiv \tau \bmod \deg \geqslant 2, \qquad \ell(L(\xi, \eta)) = \ell(\xi) + \ell(\eta).$$

One calls $\ell(\tau)$ the *logarithm* of the formal group law $L(\xi, \eta)$. The law is said to be *curvilinear* if the power series expansions of its logarithm involve no monomials with more than one variable. In that case one can write

$$\ell(\tau) = \sum_{n \geqslant 1} n^{-1} \beta_n \tau^n$$

with β_n a $g \times g$-matrix with entries in K, β_1 equal to the identity matrix, and τ^n denoting the transpose of the vector $(\tau_1^n, \ldots, \tau_g^n)$.

1.4. *Cartier's theory* associates with a formal group $\mathcal{G}$ over a ring K its *module of curves* $\mathcal{C}\mathcal{G}$

$$\mathcal{C}\mathcal{G} = \varprojlim_{n} \mathcal{G}(tK[t]/(t^n))$$

A coordination of $\mathcal{G}$ gives an identification of $\mathcal{C}\mathcal{G}$ with the set $(tK[[t]])^{\times g}$ of g-tuples of formal power series in one variable without constant term; here $g = \dim \mathcal{G}$. The addition rule on this set is provided by the formal group law attached to the coordinatization of $\mathcal{G}$.

1.5. For every positive integer n one has two operators F_n (Frobenius) and V_n (Verschiebung) acting on $\mathcal{C}\mathcal{G}$ as follows. V_n is induced by the substitution $t \mapsto t^n$. The defining formula for the action of F_n is

$$F_n(\gamma(t)) = \gamma(\zeta t^{1/n}) \boxplus \gamma(\zeta^2 t^{1/n}) \boxplus \cdots \boxplus \gamma(\zeta^n t^{1/n}),$$

for $\gamma(t) \in \mathcal{C}\mathcal{G}$; here ζ is a primitive n-th root of unity. Notice the relations

$$V_n V_m = V_{nm} \quad \text{and} \quad F_n F_m = F_{nm} \quad \text{for all} \quad n, m,$$

$$F_n V_n = nI \quad \text{for all} \quad n (I = \text{identity operator}),$$

$$V_p F_p = F_p V_p \quad \text{if} \quad K \text{ has characteristic } p, \qquad p \text{ prime},$$

$$V_n F_m = F_m V_n \quad \text{if} \quad gcd(m, n) = 1.$$

THEOREM 1.6. *Let $\mathcal{G}$ be a g-dimensional formal group over a $\mathbf{Z}$-flat ring K. Let p be a prime number and let $\mathcal{P}$ be an ideal in K which contains p. Fix an integer e such that $1 \leqslant e \leqslant p - 1$ and $p \in \mathcal{P}^e$. Let $\bar{\mathcal{G}}$ be the restriction of the functor $\mathcal{G}$ to the subcategory $\mathcal{N}il\mathcal{A}lgs_{K/\mathcal{P}}$ of $\mathcal{N}il\mathcal{A}lgs_K$. So $\bar{\mathcal{G}}$ is a formal group over $K/\mathcal{P}$. Assume one has a curvilinear formal group law for $\mathcal{G}$ with logarithm*

$$\ell(\tau) = \sum_{n \geqslant 1} n^{-1} \beta_n \tau^n,$$

and integers $k \geqslant r \geqslant 0$ and $b_1, \ldots, b_k \in \mathbf{Z}$ such that the operator

$$F_p^{\,r} + b_1 F_p^{\,r-1} + \cdots + b_{r-1} F_p + b_r I + b_{r+1} V_p + \cdots + b_k V_p^{\,k-r}$$

vanishes on $\mathcal{C}\bar{\mathcal{G}}$. Put

$$a_i = b_i \ \textit{for} \ \ 1 \leqslant i \leqslant r, \qquad a_i = p^{i-r} b_i \ \textit{for} \ \ r \leqslant i \leqslant k.$$

Then one has the following congruences:

$$\beta_{np^r} + a_1 \beta_{np^r-1} + a_2 \beta_{np^r-2} + \cdots + a_k \beta_{np^r-k} \equiv 0 \bmod \mathcal{P}^{ev+1}$$

if $n \equiv 0 \bmod p^v$. (convention: $\beta_m = 0$ if $m \notin \mathbf{Z}$; the congruence means that the left-hand side is a $g \times g$-matrix with entries in $\mathcal{P}^{ev+1}$.)

Proof. Using the coordinatization of $\mathcal{G}$ corresponding to the given formal group law we identify $\mathcal{C}\mathcal{G}$ with $(tK[[t]])^{\times g}$. By restriction from $\mathcal{N}ilalgs_K$ to $\mathcal{N}ilalgs_{K/\mathcal{P}}$ one obtains a coordinatization of $\bar{\mathcal{G}}$ and hence an identification of $\mathcal{C}\bar{\mathcal{G}}$ with $(t(K/\mathcal{P})[[t]])^{\times g}$. The kernel of $\mathcal{C}\mathcal{G} \to \mathcal{C}\bar{\mathcal{G}}$ is thereby identified with $(t\mathcal{P}[[t]])^{\times g}$. The hypothesis that $F_p^r + \cdots + b_k V_p^{k-r}$ vanishes on $\mathcal{C}\bar{\mathcal{G}}$, implies that, when this operator acts on $\mathcal{C}\mathcal{G}$, its image lies in $\ker(\mathcal{C}\mathcal{G} \to \mathcal{C}\bar{\mathcal{G}})$. In particular, writing t_i for the transpose of the vector $(0, . ., 0, t, 0, . ., 0)$ with t as i-th coordinate, we have

$$(F_p^r + b_1 F_p^{r-1} + \cdots + b_k V_p^{k-r})(t_i) = f(t) \in (t\mathcal{P}[[t]])^{\times g}.$$

To this relation we apply the logarithm ℓ. Easy computation shows that it then becomes

$$\sum_{n\geqslant 1} (\beta_{np^r} + b_1\beta_{np^{r-1}} + \cdot\cdot + b_r\beta_n + pb_{r+1}\beta_{n/p} + \cdot\cdot + p^{k-r}b_k\beta_{np^{r-k}})\frac{t_i^n}{n}$$

$$\text{equals} \quad \sum_{n\geqslant 1} n^{-1}\beta_n(f(t))^n.$$

The latter obviously is a g-tuple of power series with coefficients in the algebra $\{x \in K \otimes \mathbf{Q} \mid \text{if } nx \in K \text{ and } n \in p^v\mathbf{Z} \subset \mathbf{Z} \text{ then } nx \in \mathcal{P}^{ev+1}\}$. This proves the congruences for the i-th matrix columns. □

2. The formal groups of Artin and Mazur [1]. In this section we define the formal groups to which we want to apply theorem (1.6).

2.1. We denote the 1-*dimensional formal multiplicative group* by $\hat{\mathbf{G}}_m$. It is defined over $\mathbf{Z}$ and it admits a coordinatization so that the corresponding formal group law is $\xi + \eta - \xi\eta$, with logarithm $\Sigma_{n\geqslant 1} n^{-1}\tau^n$.

2.2. Let $\mathcal{X}$ be a scheme over a ring K, with structure sheaf $\mathcal{O}_{\mathcal{X}}$. For a nil-$K$-algebra A we construct the sheaf $\hat{\mathbf{G}}_{m,\mathcal{X}}(A)$ of abelian groups on $\mathcal{X}$ by sheafifying the pre-sheaf (Zariski open $U \subset \mathcal{X}$) $\mapsto \hat{\mathbf{G}}_m(\Gamma(U, \mathcal{O}_{\mathcal{X}}) \otimes_K A)$. The *N-th Artin-Mazur functor*

$$H^N(\mathcal{X}, \hat{\mathbf{G}}_{m,\mathcal{X}}) : \mathcal{N}ilalgs \to \mathcal{A}belian\ groups$$

(denoted Φ^N in [1]) is the functor which assigns to a nil-K-algebra A the cohomology group $H^N(\mathcal{X}, \hat{\mathbf{G}}_{m,\mathcal{X}}(A))$.

This functor is *not always a formal group.* Therefore we often have to impose the condition that $H^N(\mathfrak{X}, \hat{\mathbf{G}}_{m,\mathfrak{X}})$ is a formal group for the N we are interested in. In section 4 we give examples of schemes for which the condition is satisfied.

2.3. If $H^N(\mathfrak{X}, \hat{\mathbf{G}}_{m,\mathfrak{X}})$ is a formal group and K is a field, then the dimension of this formal group is equal to $\dim_K H^N(\mathfrak{X}, \mathcal{O}_{\mathfrak{X}})$.

2.4. Let $\mathfrak{X}$ be a flat noetherian scheme over a ring K and let $\mathcal{P}$ be an ideal in K. Put $\mathfrak{X}_{\mathcal{P}} = \mathfrak{X} \times_{\mathrm{spec}\, K} \mathrm{spec}(K/\mathcal{P})$. Then, for every N, $H^N(\mathfrak{X}_{\mathcal{P}}, \hat{\mathbf{G}}_{m,\mathfrak{X}_{\mathcal{P}}})$ is canonically isomorphic with the restriction of $H^N(\mathfrak{X}, \hat{\mathbf{G}}_{m,\mathfrak{X}})$ to $\mathcal{N}il\mathcal{a}lg\mathcal{s}_{K/\mathcal{P}}$; see [17] (3.9). In particular, if $H^N(\mathfrak{X}, \hat{\mathbf{G}}_{m,\mathfrak{X}})$ for some N is a formal group over K, then $H^N(\mathfrak{X}_{\mathcal{P}}, \hat{\mathbf{G}}_{m,\mathfrak{X}_{\mathcal{P}}})$ is a formal group over $K/\mathcal{P}$.

So the passage in (1.6) from characteristic 0 to characteristic p can be made with the Artin-Mazur formal groups.

2.5. Let K be a field and let $\pi : X \rightarrow Y$ be a morphism of schemes over K with $R^i\pi_*\mathcal{O}_X = 0$ for $i \geqslant 1$ and $\pi_*\mathcal{O}_X = \mathcal{O}_Y$. Then π induces a functorial isomorphism $H^N(X, \hat{\mathbf{G}}_{m,X}) \simeq H^N(Y, \hat{\mathbf{G}}_{m,Y})$, for every N; see [17] (3.10).

This result is useful if one can take X to be smooth. The condition then means that the singularities of Y are not too bad; e.g. rational singularities on a surface. One needs this possibility of passing from a singular model to a smooth one without changing $H^N\hat{\mathbf{G}}_m$, if one wants to exploit the connection between the Artin-Mazur formal groups and zeta-functions. This connection, which is explained in the next section, runs via the theory of the De Rham-Witt complex and crystalline cohomology, which has only been sufficiently worked out for smooth projective varieties. On the other hand, one should not insist on having a smooth scheme to begin with, since explicit logarithms of formal group laws for the Artin-Mazur formal groups are sometimes easier to compute on a model with singularities (see section 4).

3. Curves on Artin-Mazur formal groups and zeta functions. In this section we explain how one can obtain the characteristic p part of the input data for application of theorem (1.6). The main result is stated in theorem (3.12). Throughout this section X is a smooth projective variety over the finite field $\mathbf{F}_q$ of characteristic p; $q = p^f$.

3.1. If $H^N(X, \hat{\mathbf{G}}_{m,X})$ is a formal group (over $\mathbf{F}_q$), its module of curves, $\mathcal{C}(H^N(X, \hat{\mathbf{G}}_{m,X}))$, is equal to $H^N(X, \mathcal{C}\hat{\mathbf{G}}_{m,X})$ with

$$\mathcal{C}\hat{\mathbf{G}}_{m,X} = \varprojlim_n \hat{\mathbf{G}}_{m,X}(t\mathbf{F}_q[t]/(t^n)).$$

The sheaf $\mathcal{C}\hat{\mathbf{G}}_{m,X}$ is the *sheaf of generalized Witt vectors on X* (cf. [5, 4, 10]).

3.2. Let μ denote the Möbius function on $\mathbf{N}$: $\mu(1) = 1$, $\mu(n) = (-1)^r$ if n is squarefree and divisible by r primes, $\mu(n) = 0$ if n is divisible by a square >1. Then the operator

$$E = \sum_{n \in \mathbf{N} \setminus p\mathbf{N}} n^{-1}\mu(n) V_n F_n,$$

which acts on $\mathcal{C}\hat{\mathbf{G}}_{m,X}$ and on $H^N(X, \mathcal{C}\hat{\mathbf{G}}_{m,X})$, is idempotent (cf. [4, 5, 10]). The factor which it splits off from $\mathcal{C}\hat{\mathbf{G}}_{m,X}$, is the sheaf $\mathcal{W}\mathcal{O}_X$ of *p-typical Witt vectors* on X (ibid.). In $H^N(X, \mathcal{C}\hat{\mathbf{G}}_{m,X})$ it gives $H^N(X, \mathcal{W}\mathcal{O}_X)$. One even has an isomorphism

$$(*) \qquad \begin{tikzcd} H^N(X, \mathcal{C}\hat{\mathbf{G}}_{m,X}) \arrow[r, shift left=1.5, "(E_0F_n)_n"] \arrow[r, phantom, "\sim"] & \prod_n H^N(X, \mathcal{W}\mathcal{O}_X), \arrow[l, shift left=1.5, "\Sigma n^{-1}V_n"] \end{tikzcd}$$

with n running through the set $\mathbf{N}\setminus p\mathbf{N}$ (ibid.).

3.3. The operators F_p and V_p commute with all F_n and V_n for n prime to p. They also commute with E. So F_p and V_p act on $\mathcal{W}\mathcal{O}_X$ and on $H^N(X, \mathcal{W}\mathcal{O}_X)$. This action is compatible with the decomposition (*) in (3.2). In particular, an operator $F_p{}^r + b_1F_p{}^{r-1} + \cdots + b_rI + \cdots + b_kV_p{}^{k-r}$ vanishes on $H^N(X, \mathcal{C}\hat{\mathbf{G}}_{m,X})$ if and only if it vanishes on $H^N(X, \mathcal{W}\mathcal{O}_X)$. Such a vanishing operator is the essential part of the characteristic p input data for theorem (1.6), if $H^N(X, \hat{\mathbf{G}}_{m,X})$ is a formal group. We are going to construct such an operator in (3.4)-(3.11).

3.4. We now recall some facts about crystalline cohomology. References are [4, 10, 11, 12]. According to Bloch, Deligne and Illusie the *crystalline cohomology $H^*_{cris}(X)$* of X can be obtained as the hypercohomology of a complex of sheaves for the Zariski topology on X:

$$H^N_{cris}(X) = \mathbf{H}^N(X, \mathcal{W}\Omega^\cdot_X)$$

for $0 \leqslant N \leqslant 2 \dim X$. The complex $\mathcal{W}\Omega^\cdot_X$is called the *De Rham-Witt complex* on X. It is concentrated in nonnegative degrees and its degree 0 term is the sheaf $\mathcal{W}\mathcal{O}_X$ of p-typical Witt vectors on X. So there is a homomorphism $\mathcal{W}\Omega^\cdot_X \rightarrow \mathcal{W}\mathcal{O}_X$ and this induces a homomorphism

$$\varphi : \mathbf{H}^N(X, \mathcal{W}\Omega^\cdot_X) \rightarrow H^N(X, \mathcal{W}\mathcal{O}_X)$$

for $N = 0, 1, . ., \dim X$. This homomorphism appears also as the composite

$$\mathbf{H}^N(X, \mathcal{W}\Omega^\cdot_X) \twoheadrightarrow E_\infty^{0N} \hookrightarrow E_1^{0N} = H^N(X, \mathcal{W}\mathcal{O}_X)$$

in the so-called *slope spectral sequence*

$$(sss) \qquad E_1^{ij} = H^j(X, \mathcal{W}\Omega^i_X) \Rightarrow \mathbf{H}^*(X, \mathcal{W}\Omega^\cdot_X)$$

(see [4, 10, 11, 12]). The slope spectral sequence degenerates modulo torsion at $E_1^{\cdot\cdot}$ (ibid.), i.e. the differentials in the spectral sequence $(sss) \otimes \mathbf{Q}$ are zero. In particular the map

$$\varphi \otimes \mathbf{Q} : \mathbf{H}^N(X, \mathcal{W}\Omega^\cdot_X) \otimes \mathbf{Q} \rightarrow H^N(X, \mathcal{W}\mathcal{O}_X) \otimes \mathbf{Q}$$

is surjective for every N.

3.5. On the De Rham-Witt complex $\mathcal{W}\Omega^\cdot_X$one can construct a *Frobenius* endomorphism F_p, which in degree 0 coincides with the Frobenius endomorphism F_p on $\mathcal{W}\mathcal{O}_X$, as defined in (3.3) (see [4, 10, 11]). This induces Frobenius endomorphisms F_p on $\mathbf{H}^N(X, \mathcal{W}\Omega^\cdot_X)$ and $H^N(X, \mathcal{W}\mathcal{O}_X)$. On the latter it coincides with the operator F_p of (3.3). Obviously, F_p commutes with the map φ of (3.4). Since moreover $\varphi \otimes \mathbf{Q}$ is surjective, we see that, if an operator of the form $F_p^k + a_1F_p^{k-1} + \cdots + a_kI$, with $a_1, . . ., a_k \in \mathbf{Z}$, vanishes on $H^N_{cris}(X) \otimes \mathbf{Q}$, it vanishes also on $H^N(X, \mathcal{W}\mathcal{O}_X) \otimes \mathbf{Q}$.

3.6. The *zeta function* of $X/\mathbf{F}_q$ is, by definition,

$$Z(X/\mathbf{F}_q;\ T) = \exp(\sum_{n \geqslant 1} n^{-1}N_nT^n)$$

with N_n = the number of points on X defined over $\mathbf{F}_{q^n}$. By Deligne [7] and Katz-Messing [13] one knows

$$Z(X/\mathbf{F}_q;\ T) = \prod_{N=0}^{2\dim X} P_N(T)^{(-1)^{N+1}}$$

with $P_N(T) = \det(1 - TF_q \,|\, H^N_{cris}(X) \otimes \mathbf{Q})$, $P_N(T) \in \mathbf{Z}[T]$; F_q is the appropriate Frobenius endomorphism, $F_q = F_p^f$ with F_p as in (3.5). Put

$$P_N(T) = a_0 + a_1 T + \cdots + a_k T^k;$$

so $a_0, \ldots, a_k \in \mathbf{Z}$, $a_0 = 1$ and k is equal to the N-th Betti number of X. Then, by Cayley-Hamilton, the operator

$$F_q^k + a_1 F_q^{k-1} + \cdots + a_k I$$

vanishes on $H^N_{cris}(X) \otimes \mathbf{Q}$, and hence also on $H^N(X, \mathcal{W}\mathcal{O}_X) \otimes \mathbf{Q}$ (cf. (3.5.)).

3.7. Let $P_N(T)$ be as in (3.6). Write, for $a \in \mathbf{Z}$, $\operatorname{ord}_p(a) = \nu$ if $a \in p^\nu \mathbf{Z} \backslash p^{\nu+1}\mathbf{Z}$. Define

$$m = \min\{n \in \mathbf{Z} \,|\, fn \geqslant fj - \operatorname{ord}_p(a_j) \text{ for } j = 1, \ldots, k\}$$

Then $0 \leqslant m \leqslant k$ and there exist integers $c_0, \ldots, c_k$ such that

$$a_j = c_j \qquad \text{for} \quad 0 \leqslant j \leqslant m$$

$$a_j = q^{j-m} c_j \quad \text{for} \quad m \leqslant j \leqslant k.$$

Now recall that on $H^N(X, \mathcal{W}\mathcal{O}_X)$ one also has the operator $V_q = V_p^f$ and that $V_q F_q = F_q V_q = qI$. Thus

$$F_q^m + c_1 F_q^{m-1} + \cdots + c_m I + c_{m+1} V_q + \cdots + c_k V_q^{k-m}$$

$$= q^{m-k} V_q^{k-m} (F_q^k + a_1 F_q^{k-1} + \cdots + a_k I)$$

and, by (3.6), this operator acts trivially on $H^N(X, \mathcal{W}\mathcal{O}_X) \otimes \mathbf{Q}$.

3.8. Let p-tors mean the module of p-torsion elements in $H^N(X, \mathcal{W}\mathcal{O}_X)$. Then $H^N(X, \mathcal{W}\mathcal{O}_X)/(p\text{-tors})$ injects into $H^N(X, \mathcal{W}\mathcal{O}_X) \otimes \mathbf{Q}$. The operator $F_q{}^m + c_1 F_q{}^{m-1} + \cdots + c_k V_q{}^{k-m}$, constructed in (3.7), acts therefore trivially on $H^N(X, \mathcal{W}\mathcal{O}_X)/(p\text{-tors})$.

We want, however, an operator of this sort which vanishes on $H^N(X, \mathcal{W}\mathcal{O}_X)$, not just modulo torsion. For that purpose we are going to investigate the action of F_p on p-tors.

3.9. First we need more information about the integer m, defined in (3.7). The *Newton polygon* of the polynomial $P_N(T)$ is by definition the highest convex polygonal curve in $\mathbf{R}^2$ between the points $(0, 0)$ and $(k, \operatorname{ord}_p a_k)$ which passes through or below the points $(j, \operatorname{ord}_p a_j)$ for $j = 0, 1, . ., k$. Since the base field is $\mathbf{F}_q$, the Newton polygon of $P_N(T)$ coincides with the Newton polygon for the action of F_q on $H^N_{cris}(X) \otimes \mathbf{Q}$ (cf. [14]). Dividing all its slopes by f, leaving the multiplicities unchanged, one obtains the Newton polygon for the action of F_p on $H^N_{cris}(X) \otimes \mathbf{Q}$. The integer m can now be characterized geometrically by the fact that in $\mathbf{R}^2$ the line of slope 1 through the point $(0, m)$ is the lowest line of slope 1 which intersects the Newton polygon of F_p. This shows that m is equal to the *slope number* m^{0N}, defined in [12] (6.2).

Formula (6.2.6) of op. cit. yields therefore

$$m = \dim_{\mathbf{F}_q} H^N(X, \mathcal{W}\mathcal{O}_X)/(p\text{-tors} + V_p H^N(X, \mathcal{W}\mathcal{O}_X)).$$

3.10. From now on we assume that $H^N(X, \hat{\mathbf{G}}_{m,X})$ is a formal group over $\mathbf{F}_q$ of dimension g. Then

$$g = \dim_{\mathbf{F}_q} H^N(X, \mathcal{O}_X) = \dim_{\mathbf{F}_q}(H^N(X, \mathcal{W}\mathcal{O}_X)/V_p H^N(X, \mathcal{W}\mathcal{O}_X)).$$

Combining this formula for g with the formula for m given in (3.9) we see

$$g - m = \dim_{\mathbf{F}_q}((p\text{-tors})/V_p(p\text{-tors})).$$

On $((p\text{-tors})/V_p(p\text{-tors}))$ there is an increasing filtration by the $\mathbf{F}_q$-vector spaces $(\ker p^n)/((\ker p^n) \cap V_p(p\text{-tors}))$, $n = 1, 2, ...$ This sequence stabilizes at $n = g - m$, or earlier. So, V_p-adically every element of p-tors is the limit of a sequence of elements of $\ker p^{g-m}$. Since $H^N(X, \mathcal{W}\mathcal{O}_X)$ is V_p-adically complete and separated, we see

$$p\text{-tors} = \ker(p^{g-m} | H^N(X, \mathcal{W}\mathcal{O}_X)).$$

Since $H^N(X, \hat{\mathbf{G}}_{m,X})$ is a formal group, V_p acts injectively on its Cartier module, whence also on $H^N(X, \mathcal{W}\mathcal{O}_X)$. Moreover, $V_pF_p = F_pV_p = pI$. We conclude that $F_p{}^{g-m}$ vanishes on p-tors.

3.11. We combine the results of (3.8) and (3.10) by means of the exact sequence

$$0 \to (p\text{-tors}) \to H^N(X, \mathcal{W}\mathcal{O}_X) \to (H^N(X, \mathcal{W}\mathcal{O}_X)/(p\text{-tors})) \to 0.$$

In (3.8) we constructed an operator which vanishes on the right-hand term. In (3.10) we showed that F_p^{g-m} vanishes on p-tors. The product of these operators then acts trivially on $H^N(X, \mathcal{W}\mathcal{O}_X)$.

This proves:

THEOREM 3.12. *Let X be a smooth projective variety over $\mathbf{F}_q$, $q = p^f$, p prime. Assume that $H^N(X, \hat{\mathbf{G}}_{m,X})$ is a formal group over $\mathbf{F}_q$. Let*

$$P_N(T) = a_0 + a_1T + \cdots + a_kT^k = \det(1 - TF_q | H^N_{cris}(X) \otimes \mathbf{Q});$$

so, $k = N$-th Betti number of X, $a_0, \ldots, a_k \in \mathbf{Z}$, $a_0 = 1$.

Put

$$g = \dim_{\mathbf{F}_q} H^N(X, \mathcal{O}_X) = \text{dimension of } H^N(X, \hat{\mathbf{G}}_{m,X}),$$

$$m = \min\{n \in \mathbf{Z} | fn \geqslant fj - \text{ord}_p(a_j) \text{ for } 0 \leqslant j \leqslant k\},$$

$$r = g - m + fm,$$

$$t = (\text{largest integer} \leqslant (r/f)).$$

Define $b_0, \ldots, b_k \in \mathbf{Z}$ by

$$a_j = b_j \quad \text{for} \quad j = 0, \ldots, t,$$

$$a_j = p^{fj-r}b_j \quad \text{for} \quad j = t + 1, \ldots, k.$$

Then the operator

$$F_p{}^r + b_1F_p{}^{r-f} + \cdots + b_tF_p{}^{r-ft} + b_{t+1}V_p^{ft-r+f} + \cdots + b_kV_p^{fk-r}$$

vanishes on $H^N(X, \mathcal{W}\mathcal{O}_X)$, and hence, by (3.3), also on the Cartier module $\mathcal{C}(H^N(X, \hat{\mathbf{G}}_{m,X}))$ of the formal group $H^N(X, \hat{\mathbf{G}}_{m,X})$. □

3.13. The above theorem provides the characteristic p input data for application of theorem (1.6). Notice that the indices are slightly different from those in (1.6), due to the fact that in this section the natural Frobenius operator was F_q. When the resulting congruence is formulated in terms of formal Dirichlet series (cf. (0.1)), theorem (3.12) contributes the Dirichlet series

$$1 + a_1 q^{-s} + a_2 q^{-2s} + \cdots + a_k q^{-ks} = P_N(q^{-s}).$$

The congruences which result from the theorems (3.12) and (1.6) are slightly stronger than those stated in theorem (0.1). Indeed, we actually proved, in the notation of (0.1),

$$\theta_n \equiv 0 \bmod \mathcal{P}^{e(\nu-g+m-fm)+1} \quad \text{if} \quad n \equiv 0 \bmod p^\nu, \qquad \nu \geqslant g - m + fm.$$

We have ignored this when stating (0.1), because it is difficult to determine the integer m a priori.

4. Double coverings of $\mathbf{P}^N$.

In [17] we give examples of schemes for which $H^N(X, \hat{\mathbf{G}}_{m,X})$ is a formal group and for which a logarithm of a curvilinear formal group law for $H^N(X, \hat{\mathbf{G}}_{m,X})$ can explicitly be determined. Such examples provide the characteristic 0 input data for application of theorem (1.6). The examples discussed in [17], are N-dimensional complete intersections, with degree restrictions, in $\mathbf{P}^M$ and branched double coverings of $\mathbf{P}^N$. The results one gets, are very similar. Here we shall only formulate the result for double coverings of $\mathbf{P}^N$.

THEOREM 4.1. (= th. 2 of [17]). *Let K be a ring which is flat and of finite type over $\mathbf{Z}$. Let N be a positive integer. Let R be a homogeneous polynomial in $K[T_0, \ldots, T_N]$ of degree $2d > 2N$, and let X be the branched double covering of $\mathbf{P}_K^N$ defined by the equation $U^2 = R$ (where U is a new variable of weight d). Put*

$$J = \{i = (i_0, \ldots, i_N) \in \mathbf{Z}^{N+1} \mid i_0, \ldots, i_N \geqslant 1, i_0 + \cdots + i_N = d\}.$$

Then $H^N(X, \hat{\mathbf{G}}_{m,X})$ is a formal group over K of dimension

$$g = \binom{d-1}{N}$$

and there is a curvilinear formal group law for this formal group with logarithm

$$\ell(\tau) = \sum_{n \geqslant 1} n^{-1}\beta_n \tau^n$$

in which β_n is the $g \times g$ zero matrix for even n, while for odd n β_n is the $g \times g$-matrix, with rows and columns indexed by the elements of the set J, such that the entry in row i and column j is

$$\beta_{n,i,j} = \text{the coefficient of } T_0^{nj_0 - i_0} \cdot \ . \ . \ \cdot T_N^{nj_N - i_N} \quad \text{in} \quad R^{(n-1)/2}.$$

□

RIJKSUNIVERSITEIT UTRECHT

REFERENCES

[1] M. Artin and B. Mazur, Formal groups arising from algebraic varieties, *Ann. Sci. Éc. Norm. Super.*, **10** (1977), 87-132.

[2] A. Atkin and H. Swinnerton-Dyer, Modular forms on non congruence subgroups, *Proc. Symp. Pure Math. vol. XIX, Amer. Math. Soc.*, Providence 1971.

[3] F. Beukers, *Une formule explicite dans la théorie des courbes elliptiques*, preprint, Leiden 1984.

[4] S. Bloch, Algebraic K-theory and crystalline cohomology, *Publ. Math. IHES 47* (1977), 187-268.

[5] P. Cartier, Groupes formels associés aux anneaux de Witt généralisés, resp. Modules associés à un groupe formel commutatif. *Courbes typiques, C. R. Acad. Sc. Paris* **265** (1967), 49-52 resp. 129-132.

[6] ———, *Groupes formels, fonctions automorphes et fonctions zêta des courbes elliptiques, Actes du Congrès Int. Math.* Nice 1970, Tome 2: 290-299, (1971) Paris, Gauthiers-Villars.

[7] P. Deligne, La conjecture de Weil I, *Publ. Math. IHES 43* (1973), 273-307.

[8] M. Hazewinkel, *Formal Groups and Applications*, New York, Academic Press 1978.

[9] T. Honda, On the theory of commutative formal groups, *J. Math. Soc. Japan*, **22** (1970), 213-246.

[10] L. Illusie, Complexe de De Rham-Witt et cohomologie cristalline, *Ann. Éc. Norm. Super.*, **12** (1979), 501-661.

[11] ______, Complexe de De Rham-Witt, *Astérisque* **63** (1979), 83-112.

[12] ______, Finiteness, duality and Künneth theorems in the cohomology of the De Rham-Witt complex, in *Algebraic Geometry, Lecture Notes in Math.* **1016**, (1983) Berlin, Springer Verlag.

[13] N. Katz and W. Messing, Some consequences of the Riemann hypothesis for varieties over finite fields, *Inv. Math.*, **23** (1974), 73-77.

[14] N. Katz, Slope filtration of F-crystals, *Astérisque* **63** (1979), 113-164.

[15] M. Lazard, Commutative formal groups, *Lecture Notes in Math*, **443** (1975) Berlin, Springer Verlag.

[16] J. Stienstra and F. Beukers, On the Picard-Fuchs equation and the formal Brauer group of certain elliptic K3-surfaces, *Math. Ann.*, **271** (1985), 269-304.

[17] J. Stienstra, Formal group laws arising from algebraic varieties, to appear in Amer J. Math.

[18] T. Zink, Cartiertheorie kommutativer formaler Gruppen, *Teubner Texte zur Math. Band* **68**, Leipzig, Teubner Verlagsgesellschaft 1984.

[19] E. Ditters, Sur les congruences d'Atkin et de Swinnerton-Dyer, *C. R. Acad. Sc. Paris t.*, **282** (1976), 1131-1134.

[20] W. Hill, Formal groups and zeta functions of elliptic curves, *Inv. Math.*, **12** (1971), 321-336.

[21] T. Honda, Formal groups and zeta functions, *Osaka J. Math.*, **5** (1968), 199-213.

[22] N. Katz, *Travaux de Dwork*, Seminaire Bourbaki 1971/72 exp. 409, *Lecture Notes in Math.* **317**, (1973) Berlin, Springer Verlag.

[23] ______, *Crystalline Cohomology, Dieudonné Modules and Jacobi Sums*, Automorphic Forms, Representation Theory and Arithmetic, Bombay 1979, Tata Institute of Fundamental Research; Berlin etc.: Springer Verlag 1981.

[24] ______, Internal reconstruction of the unit-root F-crystal via expansion coefficients, *Ann. Sci. Éc. Norm. Super.*, **18** (1985), 245-268.

[25] T. Oda, Formal groups attached to elliptic modular forms, *Inv. Math.*, **61** (1980), 81-102.

[26] A. Scholl, Modular forms and De Rham cohomology; Atkin-Swinnerton-Dyer congruences, *Inv. Math.*, **79** (1985), 49-77.