TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 357, Number 3, Pages 901–964
S 0002-9947(04)03715-8
Article electronically published on October 19, 2004

GEOMETRY OF FERMAT ADELES

ALEXANDRU BUIUM

ABSTRACT. If $L(a,s) := \sum_n c(n,a)n^{-s}$ is a family of "geometric" $L-$functions depending on a parameter a, then the function $(p,a) \mapsto c(p,a)$, where p runs through the set of prime integers, is not a rational function and hence is not a function belonging to algebraic geometry. The aim of the paper is to show that if one enlarges algebraic geometry by "adjoining a Fermat quotient operation", then the functions $c(p,a)$ become functions in the enlarged geometry at least for $L-$functions of curves and Abelian varieties.

1. INTRODUCTION

Our starting point is the following formula for the Legendre symbol $\left(\frac{a}{p}\right)$ as a function of p and a (cf. [8]):

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}\left(1+\sum_{k=1}^{\infty}(-1)^{k-1}\frac{(2k-2)!p^k}{2^{2k-1}(k-1)!k!}(\delta_p a)^k a^{-pk}\right). \tag{1.1}$$

Here a is any integer, p is an odd prime number not dividing a, $\delta_p a := (a-a^p)/p$ is the "Fermat quotient of a with respect to p", and the right-hand side of (1.1) is viewed as an element of $\mathbf{Z}_p$, the ring of $p-$adic numbers. The proof of (1.1) is, of course, trivial: the right-hand side is $\equiv a^{\frac{p-1}{2}} \bmod p$ and its square equals $a^{p-1}(1+p(\delta_p a)a^{-p}) = 1$. Note that the right-hand side of (1.1) continues to make sense if the integer a is replaced by any element in a finite unramified extension of $\mathbf{Z}_p$ (provided the Fermat quotient $\delta_p a$ is defined by the formula $\delta_p a := (\phi(a)-a^p)/p$, where ϕ is the Frobenius automorphism); we would like to interpret this property by saying that the right-hand side of (1.1) has a "geometric" character.

Now is the formula (1.1) a mere curious fact or is it an instance of a broader principle? One (easy) way to generalize (1.1) is to consider arbitrary power residue symbols (Kummer theory), as we shall see. Another way to generalize (1.1) is to recall that the Legendre symbol belongs, of course, to the arithmetic of conics, and to then pass from conics to more general varieties. The main results of the present paper can be viewed as analogues of (1.1) for curves (of arbitrary genus) and for Abelian varieties. The broader picture that we propose is the following. Let $\mathbf{P}$ denote the set of prime numbers. Then the "interesting" functions

$$f : \mathbf{P} \times \mathbf{Z}^m \to \mathbf{Z}, \quad (p,a) \mapsto f(p,a) \tag{1.2}$$

Received by the editors August 16, 2000 and, in revised form, May 14, 2002.
2000 *Mathematics Subject Classification.* Primary 11G05, 11G30.
The author was partially supported by NSF grants DMS 9996078 and 0096946.

appearing in number theory (of which the Legendre symbol $f(p,a) := \left(\frac{a}{p}\right)$ is the prototype) are not polynomials in p and a; the language of algebraic geometry, which is the language of polynomials, does not cover the "truly arithmetic" functions (1.2). (More general examples of functions f that we would like to keep in mind are given by $p-$coefficients of $L-$functions of various algebraic-geometric objects depending on parameters a.) What we shall do, in this paper, will be to enlarge usual algebraic geometry by essentially "adjoining" to it *one* new operation, the "Fermat quotient operation"; then we propose a "conjectural principle" according to which the ring of functions $\mathcal{F}$ of this extended geometry "covers" many of the "interesting" functions (1.2). The ring $\mathcal{F}$ will be called the ring of *Fermat adeles*. Strictly speaking, as we shall see, in performing this "adjunction" process, two of the basic old operations on polynomials (composition of polynomials and principal parts of Laurent polynomials) cease to be defined and need to be re-postulated. However, unlike the Fermat quotient operator, these two operations belong to "classical calculus" and have nothing to do with arithmetic. So the moral of our work should be that all the arithmetic complexity of the "interesting" functions (1.2) should come from the Fermat quotient operation. By the way, the Fermat quotient operation, for a fixed p, was used in [5] as a substitute for a "derivation in the $p-$direction". The main idea, as well as the main difficulty, of the present paper is to vary p in the theory developed in [5].

The plan of the paper is the following. In Section 2 we will introduce our basic ring $\mathcal{F}$ of *Fermat adeles* and we will state our main results on Abelian varieties, curves, and power residue symbols. The strategy of our proofs will be the following. In Section 3, we shall develop, up to a convenient point, a "geometry" whose objects are families (X_p) (where X_p are formal schemes over $\mathbf{Z}_p$ and p runs through the set of all, except finitely many, primes) equipped with "Fermat structure"; such a structure will simply be a way of controlling all the p's at the same time, via the ring $\mathcal{F}$. Then, for any fixed scheme of finite type X over $\mathbf{Z}$, we will consider, in Section 4, the family $(J^r(X^{\wedge p}))$ of its $p-$jet spaces of order r introduced in [5] and we shall equip this family with a natural Fermat structure. In [5] p was fixed; we will show, in Sections 4 and 5, that one can make p vary while "staying in the Fermat category". Now it will turn out (and this will help us conclude) that the characteristic polynomials of Frobenii on an Abelian variety E are encoded into the second $p-$jet spaces $J^2(E^{\wedge p})$ of E; the strategy to prove this will be explained in Section 6. The actual proofs will be carried out in Sections 7 and 8. They will draw on the theory of differential characters [5], [7] and differential modular forms [8], [2] which will be quickly reviewed in Section 6.

2. Fermat adeles and statement of the main results

In order to define our ring $\mathcal{F}$ of Fermat adeles we will start with the ring of polynomials, $\mathcal{P}$, with integer coefficients (in infinitely many variables), we will consider its "adelization", $\mathcal{A}$, we shall define some basic operations on $\mathcal{A}$ and, finally, we shall define $\mathcal{F}$ as the smallest subring of $\mathcal{A}$ closed under these operations.

2.1. **The rings $\mathcal{P}$ and $\mathcal{A}$.** Let $x = \{x_1, x_2, x_3, ...\}$ be variables and consider the ring of polynomials

$$\mathcal{P} := \mathbf{Z}[x] = \bigcup_{n \geq 0} \mathbf{Z}[x_1, ..., x_n]$$

and its "adelization"

$$\mathcal{A} := \bigcup_{n\geq 0} \prod_{p\notin S} \mathbf{Z}_p[x_1, ..., x_n]^{\wedge p},$$

where S is a fixed finite set of rational primes and, for each prime $p \notin S$, the superscript $^{\wedge p}$ denotes "$p-$adic completion". The elements of $\mathcal{A}$ will be referred to as *adeles (outside S)*. The elements of the ring $\mathcal{A}$ will be typically viewed as families (f_p), $f_p \in \mathbf{Z}_p[x_1, ..., x_n]^{\wedge p}$, for some n that does not depend on p. Note that there is a natural (diagonal) embedding $\mathcal{P} \subset \mathcal{A}$. Also, $\mathcal{A}$ contains a distinguished element $\mathbf{p} := (p)$, the adele whose $p-$component is p. One can view $\mathcal{A}$ with its $\mathbf{p}-$adic topology. (Note that the "adelic" topology is, of course, "much" weaker than the $\mathbf{p}-$adic topology.) More generally one can consider, for all $k \geq 1$, the "divided powers" $\mathbf{p}^k/k! := (p^k/k!) \in \mathcal{A}$. Denote by $\mathcal{P}\{\mathbf{p}\}$ the $\mathcal{P}-$subalgebra of $\mathcal{A}$ generated by all divided powers $\mathbf{p}^k/k!$, for $k \geq 1$.

2.2. **Operations on $\mathcal{A}$.** We will consider a few basic operations on the ring $\mathcal{P}$. These will induce corresponding operations on $\mathcal{A}$.

1) First, for each p, there is the *Fermat quotient* operator

$$\delta_p : \mathcal{P} \to \mathcal{P}, \quad \delta_p f := \frac{f(x^p) - f(x)^p}{p}.$$

2) Next, for $k \geq 1$, there are *composition* maps

$$\gamma_k : \mathcal{P} \times \mathcal{P} \to \mathcal{P}, \quad \gamma_k(f, g) := f(x_1, ..., x_{k-1}, g, x_{k+1}, ...).$$

3) Finally, consider the *principal part* operator

$$\mathcal{P}[x_1^{-1}] \to \mathcal{P}, \quad h = \sum_{k=-d}^{\infty} a_k x_1^k \mapsto h^- := \sum_{k=0}^{d} a_{-k} x_1^k,$$

where $a_k \in \mathbf{Z}[x_2, x_3, ...]$. We have an induced *principal part* operator

$$\beta : \mathcal{P} \to \mathcal{P}, \quad \beta(f(x_1, x_2, x_3, ...)) := (f(x_1^{-1}, x_1, x_2, ...))^-.$$

Now the maps $\delta_p, \gamma_k, \beta$ preserve $\mathbf{Z}[x_1, ..., x_n]$ for each n so, extending these maps by continuity to $\mathbf{Z}_p[x_1, ..., x_n]^{\wedge p}$, taking products for $p \notin S$, and letting $n \to \infty$, one gets maps

1) $\delta_{\mathbf{p}} : \mathcal{A} \to \mathcal{A}$,
2) $\gamma_k : \mathcal{A} \times \mathcal{A} \to \mathcal{A}$,
3) $\beta : \mathcal{A} \to \mathcal{A}$.

2.3. **The ring $\mathcal{F}$.** Let us consider the intermediate rings $\mathcal{P}\{\mathbf{p}\} \subset \mathcal{F} \subset \mathcal{A}$ satisfying the following conditions:

1) *Fermat quotient axiom.* $\delta_{\mathbf{p}}(\mathcal{F}) \subset \mathcal{F}$.
2) *Composition axiom.* $\gamma_k(\mathcal{F} \times \mathcal{F}) \subset \mathcal{F}$ for all $k \geq 1$.
3) *Principal part axiom.* $\beta(\mathcal{F}) \subset \mathcal{F}$.

Any intersection of rings satisfying axioms 1)-3) obviously still satisfies these axioms. Moreover, the $\mathbf{p}-$adic closure in $\mathcal{A}$ of any ring that satisfies axioms 1)-3) will satisfy axioms 1)-3) and in addition satisfies the following axiom:

4) $\mathbf{p}$*-adic closure axiom.* $\mathcal{F}$ is $\mathbf{p}-$adically closed in $\mathcal{A}$.

Definition 2.1. The ring of Fermat adeles outside S is the smallest subring of $\mathcal{A}$ that satisfies axioms 1)-4). It will be denoted from now on by $\mathcal{F}$. Alternatively $\mathcal{F}$ is the $\mathbf{p}-$adic closure in $\mathcal{A}$ of the smallest subring $\mathcal{F}_0$ of $\mathcal{A}$ that satisfies axioms 1)-3). A family $(f_p) \in \mathcal{A}$ will be called *a Fermat* family if it belongs to $\mathcal{F}$.

It is interesting to examine what happens if we remove the Fermat quotient axiom from our axioms. Indeed, the smallest subring of $\mathcal{A}$ containing $\mathcal{P}\{\mathbf{p}\}$ and satisfying axioms 2)-4) is the $\mathbf{p}-$adic closure of $\mathcal{P}\{\mathbf{p}\}$. So the operation $\delta_{\mathbf{p}}$ is, in this sense, the only "new" one. On the other hand, for evidence that $\mathcal{F}$ is reasonably "small" we refer to Remark 2.7 below.

We close our discussion of Fermat adeles by attaching (formal) $L-$functions to them. Let $\mathbf{Witt}_p$ denote the class of all complete discrete valuation rings with maximal ideal generated by p and perfect residue field $k = R/pR$. For any $R \in \mathbf{Witt}_p$ let $\phi : R \to R$ be the unique automorphism that lifts the $p-$power Frobenius on k and let $\delta : R \to R$ be the map defined by the formula $\delta a = (\phi(a) - a^p)/p$. For any $g \in \mathcal{F}$, any $p \notin S$, any $R \in \mathbf{Witt}_p$, and any $P \in \mathbf{A}^N(R)$, with coordinates $a \in R^N$, we write

$$g\langle P\rangle = g\langle a\rangle := g_p(a, \delta a, \delta^2 a, ...) \in R.$$

Finally, for any square matrix f with coefficients in $\mathcal{F}$, any $g \in \mathcal{F}$, any $p \notin S$, any $R \in \mathbf{Witt}_p$ with residue field of size p^d, and any $P \in \mathbf{A}^N(R)$ such that $g\langle P\rangle \in R^\times$ we may consider the matrix, with coefficients in R,

$$\gamma_P := \frac{f\langle P\rangle}{g\langle P\rangle}$$

and define the (formal) $L-$function

$$L_P(f/g, s) := [det(I - p^{-ds} \cdot (\phi^{d-1}\gamma_P) \cdot (\phi^{d-2}\gamma_P) \cdot (\phi^{d-3}\gamma_P) \cdot ... \cdot (\phi\gamma_P) \cdot \gamma_P)]^{-1}.$$

The above expression is viewed as a formal power series in the symbol p^{-s}, with coefficients in R.

All our definitions above were relative to a fixed finite set of primes S. To emphasize this dependence write, for one moment, $\mathcal{F}^S, \mathcal{A}^S$ in place of $\mathcal{F}, \mathcal{A}$. Then if S' is a finite set of primes containing S and $pr : \mathcal{A}^S \to \mathcal{A}^{S'}$ is the natural projection, it is trivial to see that $pr(\mathcal{F}^S) \subset \mathcal{F}^{S'}$. Unless otherwise stated, S will be fixed in what follows; there will be, however, instances in which we will have to modify S.

2.4. **Main conjecture and results.** Let us describe, in what follows, the arithmetic functions that we want to "represent" with the help of the elements of $\mathcal{F}$. The following will be referred to as the *standard situation*. Assume we are given a finite set S of rational primes and a number field K with ring of integers $\mathcal{O}_K$. Assume also that we are given an affine scheme of finite type $Y/\mathcal{O}_K$ and a scheme of finite type X/Y. Assume finally that for each closed point $y \in Y$ we are given a "local $L-$function" $L_y(X/Y, s) = [det(I - N(y)^{-s} \cdot \Gamma_y)]^{-1}$, where $N(y) = p^{deg(y)}$ is the size of the residue field $\kappa(y)$ and Γ_y is some square matrix with coefficients in a field extension of K, whose characteristic polynomial has coefficients in $\mathcal{O}_K$.

We have in mind the following two basic examples:

1) (Hasse-Weil situation) We assume $Y/\mathcal{O}_K$ is smooth, Y is connected, X/Y is smooth, projective, with connected geometric fibers, and Γ_y is the matrix, with respect to some basis, of the $N(y)-$power Frobenius acting on $H^i(X_y)$. Here i is a fixed integer, $X_y := X \otimes \kappa(y)$, and H^i is either the etale ($l-$adic, l prime to $N(y)$)

or the crystalline cohomology tensored with $\mathbf{Q}$. (The etale and crystalline theories give the same $L-$functions by [18].)

2) (Artin situation) We assume X/Y is a finite Galois cover of integral normal schemes, with Galois group G, and we assume we are given a finite-dimensional complex vector space V and a representation $\rho : G \to GL(V)$ such that ρ is integral over K (i.e. the characteristic polynomials of the elements in its image have coefficients in the ring of integers $\mathcal{O}_K$). The matrices Γ_y are defined as follows. For any closed point $y \in Y$ let $x \in X$ be a closed point above y, consider the $N(y)-$power Frobenius as an element in $G(\kappa(x)/\kappa(y))$, lift this element to an element σ in the decomposition subgroup $G_x \subset G$ of x (cf. [17], p. 15), map σ into $GL(V)$ via ρ and let Γ_y be the matrix, with respect to some basis, of $\rho(\sigma)$ acting on the invariants V^{I_x} of the inertia group of x.

To state our conjecture we need one more notation. For any scheme of finite type Y over $\mathbf{Z}$ and any $R \in \mathbf{Witt}_p$ we let $Y(R)_!$ denote the set of all $R-$points of Y such that the image $y(P) \in Y$ of the closed point of $Spec\ R$ is a closed point in Y, and such that the residue field $\kappa(y)$ equals the residue field $k = R/pR$.

Conjecture. *Assume X/Y is either in the Hasse-Weil situation or in the Artin situation. Then there exists an embedding $Y \subset \mathbf{A}^N$, there exists a square matrix f with coefficients in $\mathcal{F}$ and there exists $g \in \mathcal{F}$ such that for any $p \notin S$ which splits completely in K the following hold:*

1) *There exists $R \in \mathbf{Witt}_p$ and $P \in Y(R)_!$ such that $g\langle P\rangle \in R^\times$.*
2) *For any $R \in \mathbf{Witt}_p$ and $P \in Y(R)_!$ such that $g\langle P\rangle \in R^\times$, we have*

$$L_{y(P)}(X/Y, s) = L_P(f/g, s).$$

In the above statement $L_P(f/g, s)$ is formed by identifying $Y(R)$ with a subset of $\mathbf{A}^N(R)$. Part 1) says, roughly speaking, that part 2) is a non-empty (and hence, in some sense, valid "generically") statement. In order to check part 2) in the Hasse-Weil situation it is enough, by crystalline theory, to show that $\frac{f\langle P\rangle}{g\langle P\rangle}$ coincides with the matrix, with respect to some basis, of the $p-$power Frobenius acting on the crystalline cohomology (tensored with $\mathbf{Q}$) group $H^i(X_{y(P)})$. In the Artin situation there is no general analogue of this crystalline picture, but an analogue of this exists in some interesting situations (e.g. in the "Kummer situation", as we shall see presently). Also, the conjectural picture offered above should actually be extended to include Artin $L-$functions of Galois representations that are not necessarily integral over K.

As a matter of terminology, each time we will say that the Conjecture holds for some X/Y it will be clear what situation (Hasse-Weil or Artin) we are placing ourselves in: if the fibers of X/Y are connected we are placing ourselves in the Hasse-Weil situation while if the fibers of X/Y are finite we are placing ourselves in the Artin situation.

Here are our main results for the Hasse-Weil situation. In the case of curves and Abelian varieties we prove the Conjecture holds "generically" on the moduli space:

Theorem 2.2. *Let $K = \mathbf{Q}$. For each g there exists a finite set of primes S and a curve X/Y of genus g such that the classifying map from Y to the moduli scheme of curves is etale, and such that the Conjecture holds for X/Y.*

Theorem 2.3. *Let $K = \mathbf{Q}$. For each natural number m there exists a finite set of primes S and a principally polarized Abelian scheme X/Y of relative dimension*

m such that the classifying map from Y to the moduli stack of principally polarized Abelian schemes is etale, and such that the Conjecture holds for X/Y.

In the case of elliptic curves we can be more specific.

Theorem 2.4. *Let $K = \mathbf{Q}$. There exists a finite set of primes S such that if N is the product of the primes in S, $Y = \mathbf{Z}[1/N][a_4, a_6, \Delta^{-1}]$ (where a_4, a_6 are indeterminates, $\Delta = 4a_4^3 + 27a_6^2$), and X/Y is the Weierstrass elliptic curve*

$$y^2z = x^3 + a_4xz^2 + a_6z^3,$$

then the Conjecture holds for X/Y.

The above theorem will not cover the case of CM elliptic curves: the Fermat adele g in the Conjecture will vanish, in the case of Theorem 2.4, on all CM elliptic curves. However one can prove a separate result for CM elliptic curves/Hecke characters:

Theorem 2.5. *Let K be the Hilbert class field of an imaginary quadratic field K_0. Let X/Y be elliptic curve equipped with an invertible $1-$form and with an isomorphism $\mathcal{O}_{K_0} \simeq End(X/Y)$. Then, for a suitable finite set of primes S, the Conjecture holds for X/Y.*

The families X/Y in the above Theorem are, of course, isotrivial; but this does not make them uninteresting: a typical example for the above theorem can be obtained by letting $K_0 = K = \mathbf{Q}(\zeta_3)$, letting Y be the multiplicative group $\mathbf{G}_{m,\mathbf{Z}} = Spec\ \mathbf{Z}[\zeta_3][t, t^{-1}]$ over $\mathbf{Z}[\zeta_3]$, and letting X be the elliptic curve

$$y^2z = x^3 - tz^3.$$

In the Artin situation we can successfully deal with "power residue symbols" (Kummer theory):

Theorem 2.6. *Let $K = \mathbf{Q}(\zeta_n)$ and let S be the set of all primes dividing n. Let X/Y be the multiplication by n isogeny of the multiplicative group*

$$\mathbf{G}_{m,\mathbf{Z}[\zeta_n,1/n]} \to \mathbf{G}_{m,\mathbf{Z}[\zeta_n,1/n]}$$

over $\mathbf{Z}[\zeta_n, 1/n]$. Consider the identification ρ of the Galois group G of X/Y with the group of $n-$th roots of unity in $K^\times \subset \mathbf{C}^\times$. Then the Conjecture holds for X/Y.

Let us note that in the hypothesis of Theorem 2.6 the $L-$functions can be described as follows. If $R \in \mathbf{Witt}_p$ and $P \in Y(R)_!$ corresponding to $a \in R^\times$, then take any extension R' of R in $\mathbf{Witt}_p$ containing an $n-$th root $a^{1/n}$ of a and we will have

$$\Gamma_{y(P)} = \frac{\phi^d(a^{1/n})}{a^{1/n}},$$

where p^d is the size of the residue field of R. Note that our Theorem 2.6 follows if we can find $f, g \in \mathcal{F}$ such that, for $p \equiv 1\ (n)$, and $a \in R^\times$, we have $g\langle a\rangle \in R^\times$ and

$$\frac{f\langle a\rangle}{g\langle a\rangle} = \frac{\phi(a^{1/n})}{a^{1/n}}.$$

Of course the right-hand side of the above equality, call it γ, is not a root of unity in general! One can characterize γ as the unique element in R whose $n-$th power is $\frac{\phi(a)}{a}$ and which is $\equiv$ mod p to $a^{\frac{p-1}{n}}$.

The proof of Theorem 2.6 is easy and entirely explicit; it will be completed at the end of the present section. The proofs of the rest of the theorems will occupy Sections 6-8, and will require a considerable amount of preparation, in Sections 2-5.

2.5. **Elementary consequences of the axioms and further remarks.** In what follows we derive a number of completely elementary consequences of the axioms defining the ring $\mathcal{F}$ and we also make a number of remarks. In particular, for a comparison with Ihara's viewpoint on Fermat quotients [16] we refer to Remark 2.15 below. For remarks on why various naive approaches to generalizing (1.1) do not fit into our "Fermat paradigm", and should be viewed as "non-geometric", we refer to Remarks 2.20, 2.21, 2.22 below. For a comment on the relationship between Dwork's approach [10] and ours we refer to Remark 2.23 below.

Remark 2.7. It will be useful to introduce the following notations:

$$\mathcal{P}(n) := \mathbf{Z}[x_1, ..., x_n],$$

hence $\mathcal{P}(n)^{\wedge p} = \mathbf{Z}_p[x_1, ..., x_n]^{\wedge p}$, and also

$$\mathcal{A}(n) := \prod_{p \notin S} \mathcal{P}(n)^{\wedge p},$$

$$\mathcal{F}(n) := \mathcal{F} \cap \mathcal{A}(n).$$

In what follows we provide some evidence that our ring $\mathcal{F}$ is "reasonably small". Obviously, one can construct $\mathcal{F}_0$ as an ascending union $\bigcup \mathcal{F}_0^{(m)}$ where $\mathcal{F}_0^{(0)} = \mathcal{P}\{\mathbf{p}\}$ and, for $m \geq 0$, each ring $\mathcal{F}_0^{(m+1)}$ is generated by

$$\mathcal{F}_0^{(m)}, \delta_{\mathbf{p}}(\mathcal{F}_0^{(m)}), \gamma_k(\mathcal{F}_0^{(m)} \times \mathcal{F}_0^{(m)}), \beta(\mathcal{F}_0^{(m)}).$$

This description implies that $\mathcal{F}_0$ is countable. Note also that

$$\mathcal{F}_0 \subset \bigcup_n \prod_{p \notin S} \mathbf{Z}_{(p)}[x_1, ..., x_n].$$

Now for any n and any ν there is a surjection

$$\mathcal{F}_0(n) := \mathcal{F}_0 \cap \mathcal{A}(n) \to \mathcal{F}(n)/\mathbf{p}^\nu \mathcal{A}(n) \cap \mathcal{F}(n).$$

Since $\mathcal{F}_0(n)$ is countable so is $\mathcal{F}(n)/\mathbf{p}^\nu \mathcal{A}(n) \cap \mathcal{F}(n)$. Since $\mathcal{A}(n)/\mathbf{p}\mathcal{A}(n)$ is uncountable it follows, in particular, that $\mathcal{F}(n) \neq \mathcal{A}(n)$ for all n. This observation can be refined as follows. Let $g = (g_p) \in \mathcal{F}(n)$ be such that $ord_p g_p = 0$ for infinitely many p's. (Here $ord_p g_p$ is the supremum of the set of all integers m such that p^m divides g_p in the ring $\mathcal{P}(n)^{\wedge p}$.) We claim that $\mathcal{F}(n)[g^{-1}] \neq \mathcal{A}(n)[g^{-1}]$. Indeed, we have a surjective map

$$\mathcal{F}_0(n)[g^{-1}] \to \mathcal{F}(n)[g^{-1}]/\mathbf{p}\mathcal{A}(n)[g^{-1}] \cap \mathcal{F}(n)[g^{-1}]$$

so if we assume $\mathcal{F}(n)[g^{-1}] = \mathcal{A}(n)[g^{-1}]$ we get that the map

$$\mathcal{F}_0(n)[g^{-1}] \to (\mathcal{A}(n)/\mathbf{p}\mathcal{A}(n))[g^{-1}]$$

is surjective hence $(\mathcal{A}(n)/\mathbf{p}\mathcal{A}(n))[g^{-1}]$ is countable. Let T be the set of all $p \notin S$ such that $ord_p g_p = 0$ and let $U := \prod_{p \in T}(\mathcal{P}(n)/p\mathcal{P}(n))$. Then U is uncountable and $U[\bar{g}^{-1}]$ is countable, where $\bar{g}$ is the image of g in U. By our assumption, however, $\bar{g}$ is a non-zero divisor in U so U embeds into $U[\bar{g}^{-1}]$, a contradiction.

The following remark is in order. Let us say that an element $(g_p) \in \mathcal{A}$ is *infinitely small* if $ord_p g_p \to \infty$ as $p \to \infty$. Let $\mathcal{A}_\infty$ be the set of infinitely small elements of $\mathcal{A}$; it is an ideal in $\mathcal{A}$. We will see later that $\mathcal{A}_\infty \subset \mathcal{F}$. Then, clearly, for any

$g \in \mathcal{A}_\infty \cap \mathcal{A}(n)$ we have $\mathcal{F}(n)[g^{-1}] = \mathcal{A}(n)[g^{-1}]$. Hence expressing an element of $\mathcal{A}$ as a quotient f/g of elements of $\mathcal{F}$ is only significant if we restrict g, for instance, if $ord_p g_p = 0$ for infinitely many p's. On the other hand note that if $g = (g_p)$ is the Fermat adele in our Conjecture, then, by part 1) of the Conjecture, $ord_p g_p = 0$ for all $p \notin S$ that splits completely in K, hence for infinitely many p's.

Also, we will see later that $\mathbf{p}\mathcal{A}(0) \cap \mathcal{F}(0) = \mathbf{p}\mathcal{F}(0)$; hence $\mathcal{F}(0)/\mathbf{p}^\nu \mathcal{F}(0)$ is countable for all ν.

Remark 2.8. Using the construction of $\mathcal{F}_0$ as a union $\cup \mathcal{F}_0^{(m)}$ (cf. Remark 2.7), one can easily check that any element $(f_p) \in \mathcal{F}_0$ has the property that there exists an integer $\mu \geq 0$ such that, for all $p \notin S$, f_p is a polynomial with $\mathbf{Z}_{(p)}-$coefficients, of degree $\leq p^\mu$. Consequently, any element $(f_p) \in \mathcal{F}(n)$ has the following property: for any integer $\nu \geq 0$ there exists an integer $\mu \geq 0$ such that, for all $p \notin S$, f_p is congruent mod p^ν in $\mathcal{P}(n)^{\wedge p}$ to a polynomial with $\mathbf{Z}_p-$coefficients, of degree $\leq p^\mu$.

Remark 2.9. Let us note that the Composition axiom trivially implies that for any $(f_p) \in \mathcal{F}(n)$ and any $(g_p^1), ..., (g_p^n) \in \mathcal{F}(m)$ we have $(f_p(g_p^1, ..., g_p^n)) \in \mathcal{F}(m)$. Now for any polynomial $u \in \mathcal{P}$ monic, of degree d, in x_1 we define

$$q_u, r_u : \mathcal{P} \to \mathcal{P}$$

by letting $q_u(f), r_u(f)$ be the quotient and the remainder when f is divided by u. In other words $q_u(f), r_u(f)$ are defined by the relations $f = uq_u(f) + r_u(f)$, $deg_{x_1}(r_u(f)) < d$. By continuity q_u, r_u induce maps $q_u, r_u : \mathcal{A} \to \mathcal{A}$. We claim that q_{x_k}, r_{x_k} send $\mathcal{F}$ into itself. By the Composition axiom it is enough to check this for q_{x_1}. Let $(f_p(x_1, ..., x_n)) \in \mathcal{F}(n)$, $u \in \mathcal{P}(n)$. By the Composition axiom

$$(f_p(x_1, x_3, ..., x_{n+1})x_2) \in \mathcal{F}.$$

By the Principal part axiom

$$((f_p(x_1^{-1}, x_2, ..., x_n)x_1)^-) \in \mathcal{F}.$$

But the latter family coincides with the family $(q_{x_1}(f_p))$ and we are done. An immediate consequence of this is that if $(f_p) \in \mathcal{F}(n)$, $f_p = \sum a_{ip} x_n^i$, $a_{ip} \in \mathcal{P}(n-1)^{\wedge p}$, then, for all i, we have $(a_{ip}) \in \mathcal{F}(n-1)$.

Remark 2.10. Next, for $k \geq 1$, we consider the usual partial derivative operators

$$\delta_{x_k} : \mathcal{P} \to \mathcal{P}, \quad \delta_{x_k} f := \frac{\partial f}{\partial x_k}.$$

By continuity we have induced maps

$$\delta_{x_k} : \mathcal{A} \to \mathcal{A}.$$

We claim that each δ_{x_k} sends $\mathcal{F}$ into itself. (We call this the Differentiability axiom.) It is sufficient to check this for $k = 1$. Let $(f_p(x_1, ..., x_n)) \in \mathcal{F}$. Then by the Composition axiom

$$((f_p(x_3 + x_2, x_4, ..., x_{n+2}) - f_p(x_3, x_4, ..., x_{n+2}))x_1) \in \mathcal{F}.$$

By the Principal part axiom

$$(((f_p(x_2 + x_1, x_3, ..., x_{n+1}) - f_p(x_2, x_3, ..., x_{n+1}))x_1^{-1})^-) \in \mathcal{F}.$$

But the latter equals

$$((\delta_{x_1} f_p)(x_2, x_3, ..., x_{n+1}))$$

and we conclude by the Composition axiom again.

Remark 2.11. For any n set

$$C_{p^n}(x_1, x_2) := \frac{x_1^{p^n} + x_2^{p^n} - (x_1 + x_2)^{p^n}}{p}.$$

Note that $(C_p(x_1, x_2)) \in \mathcal{F}$ because of the Fermat quotient axiom and the equality

$$C_p(x_1, x_2) = \delta_p(x_1 + x_2).$$

It follows, by the Differentiability axiom (Remark 2.10 above), that

$$(x_2^{p-1} - (x_2 + x_1)^{p-1}) = (\delta_{x_2}(C_p(x_2, x_1))) \in \mathcal{F}.$$

Setting $x_2 = 0$, by the Composition axiom, we get $(x_1^{p-1}) \in \mathcal{F}$, hence, in particular, $(x_1^p) \in \mathcal{F}$. By the Composition axiom we get $(x_1^{p^n}) \in \mathcal{F}$ for all n. Also, in particular, since $(x_1^p) \in \mathcal{F}$ we obtain, using the last property in Remark 2.9, that the adele which is 1 at one prime and 0 at all other primes belongs to $\mathcal{F}$. (Indeed, if l is a fixed prime and a_{lp} is the coefficient of x_1^l in x_1^p, then a_{lp} is either 1 or 0 according as $p = l$ or $p \neq l$; on the other hand, by the last property in Remark 2.9, we have $(a_{lp}) \in \mathcal{F}$.) In particular any element in $\mathcal{A}$ with finite support is in $\mathcal{F}$. This immediately implies that the ideal $\mathcal{A}_\infty$ of infinitely small adeles is contained in $\mathcal{F}$. As a consequence we claim that $\mathbf{p}\mathcal{A}(0) \cap \mathcal{F}(0) = \mathbf{p}\mathcal{F}(0)$. Indeed, if $(f_p) \in \mathcal{A}(0)$ and $(pf_p) \in \mathcal{F}(0)$, then $(\delta_p(pf_p)) \in \mathcal{F}(0)$. But

$$\delta_p(pf_p) = \frac{pf_p - p^p f_p^p}{p} = f_p - p^{p-1} f_p^p.$$

However $(p^{p-1} f_p^p)$ is infinitely small, so $(f_p) \in \mathcal{F}(0)$. As a consequence of the equality $\mathbf{p}\mathcal{A}(0) \cap \mathcal{F}(0) = \mathbf{p}\mathcal{F}(0)$ one gets that if $a \geq 0$ and $b \geq 1$ are integers such that $p^a/b \in \mathbf{Z}_{(p)}$ for all $p \notin S$, then $\mathbf{p}^a/b \in \mathcal{F}$. In particular if $s := \prod_{q \in S} q$, then $\mathbf{Z}_S := \mathbf{Z}[s^{-1}] \subset \mathcal{F}$. Indeed we have $\mathbf{p}^{a+b}/(a+b)! \in \mathcal{F}(0)$, hence $\mathbf{p}^b(\mathbf{p}^a/b) = \mathbf{p}^{a+b}/b \in \mathcal{F}(0)$. Since $\mathbf{p}^a/b \in \mathcal{A}(0)$ we conclude that $\mathbf{p}^a/b \in \mathcal{F}(0)$.

Remark 2.12. We claim that $(C_{p^n}(x_1, x_2)) \in \mathcal{F}$ for all n. Indeed this follows by induction from the formula

$$C_{p^{n+1}}(x_1, x_2) = p^{p^n - 1}(C_p(x_1, x_2))^{p^n} + C_{p^n}(x_1^p + x_2^p, -(x_1 + x_2)^p) + C_{p^n}(x_1^p, x_2^p)$$

together with Remark 2.11 above. As one more consequence note that

$$(\sum_{i=0}^{p^n - 1} x_1^i) \in \mathcal{F}.$$

Indeed, by the Composition axiom, it is enough to show that

$$(((x_1 + 1)^{p^n} - 1)x_1^{-1}) \in \mathcal{F}.$$

The latter equals

$$(q_{x_1}((x_1 + 1)^{p^n} - 1))$$

and we conclude by Remarks 2.11 and 2.9.

Remark 2.13. Consider the multiplicative system $\Sigma(n) \subset \mathcal{P}(n)$ of all elements in $\mathcal{P}(n)$ which become invertible in the ring of Laurent series

$$\mathbf{Z}[x_2, ..., x_n]((x_1)) := \mathbf{Z}[x_2, ..., x_n][[x_1]][x_1^{-1}].$$

Also set $\Sigma := \bigcup \Sigma(n)$. Then the ring of fractions $\mathcal{R}(n) := \Sigma(n)^{-1}\mathcal{P}(n)$ is a subring of $\mathbf{Z}[x_2, ..., x_n]((x_1))$. Similarly $\mathcal{R} := \Sigma^{-1}\mathcal{P}$ is a subring of $\bigcup \mathbf{Z}[x_2, ..., x_n]((x_1))$.

Note that $\Sigma(n)$ is generated, as monoid, by x_1, -1, and all polynomials of the form $1 - x_1 Q$, with $Q \in \mathcal{P}(n)$. Consider the "principal part" operator $h \mapsto h^-$

$$\mathcal{R}(n) \to \mathcal{P}(n)$$

that maps any $h = \sum_{k=-d}^{\infty} a_k x_1^k \in \mathcal{R}(n)$, where $a_k \in \mathbf{Z}[x_2, ..., x_n]$ into

$$h^- := \sum_{k=0}^{d} a_{-k} x_1^k.$$

Then, for any integer $1 \leq k \leq n$, we have an induced "principal part" operator

$$\beta_k : \mathcal{P}(n) \times \mathcal{R}(n)^k \to \mathcal{P}(n),$$

$$\beta_k(f, r_1, ..., r_k) := (f(r_1, ..., r_k, x_{k+1}, ..., x_n))^-.$$

By continuity we get an operator

$$\beta_k : \mathcal{A} \times \mathcal{R}^k \to \mathcal{A}$$

We claim that $\beta_k(\mathcal{F} \times \mathcal{R}^k) \subset \mathcal{F}$. (We call this the generalized Principal part axiom.) It is enough to check that $\beta_n(\mathcal{F}_0(n) \times \mathcal{R}^n) \subset \mathcal{F}$. Let $(f_p) \in \mathcal{F}_0(n)$ and $r_i = P_i x_1^{-m}(1 - x_1 Q_i)^{-1}$, $P_i, Q_i \in \mathcal{P}(n)$. By Remark 2.8, there exists an integer μ such that $deg(f_p) \leq p^\mu$. Let ν be an integer such that $p^\nu \geq m(p^\mu + 1)$ and let $r_i' = P_i x_1^{-m} s_i$, where

$$s_i := \sum_{j=0}^{p^\nu} (x_1 Q_i)^j.$$

Then it is easy to see that

$$(f_p(r_1, ..., r_n))^- = (f_p(r_1', ..., r_n'))^-.$$

The right-hand side of the above equality equals, however,

$$\beta(f_p(..., P_i(x_2, x_3, ..., x_{n+1}) x_1^m s_i(x_2, x_3, ..., x_{n+1}), ...))$$

and we conclude by the Principal part axiom, plus the last part of Remark 2.12.

Remark 2.14. Assume $u \in \mathcal{P}(n)$ is a monic polynomial, as in Remark 2.9. Note that we have the following link between $q_u : \mathcal{P}(n) \to \mathcal{P}(n)$ and the principal part operator β_k from Remark 2.13. Let $u = x_1^d + a_1 x_1^{d-1} + ... + a_d$, $a_1, ..., a_d \in \mathbf{Z}[x_2, ..., x_n]$ and set $g = 1 + a_1 x_1 + ... + a_d x_1^d$. Let $f \in \mathcal{P}(n)$. Then we have

$$q_u(f) = \left(\frac{f(x_1^{-1}, x_2, ..., x_n)}{u(x_1^{-1}, x_2, ..., x_n)} \right)^-$$

$$= \left(\frac{f(x_1^{-1}, x_2, ..., x_n) x_1^d}{g} \right)^- = \beta_{n+2}(f(x_1, ..., x_n) x_{n+1} x_{n+2}, x_1^{-1}, x_2, ..., x_n, x_1^d, g^{-1}).$$

We claim that the following "Euclidean division axiom" is satisfied: $q_u(\mathcal{F}) \subset \mathcal{F}$ and $r_u(\mathcal{F}) \subset \mathcal{F}$. Indeed, if $(f_p) \in \mathcal{F}(n)$, then

$$(F_p) := (f_p(x_1, ..., x_n) x_{n+1} x_{n+2}) \in \mathcal{F}(n+2).$$

By continuity we still have

$$q_u(f_p) = \beta_{n+2}(F_p, x_1^{-1}, x_2, ..., x_n, x_1^d, g^{-1})$$

and we conclude by the generalized Principal part axiom in Remark 2.13. This can be slightly generalized as follows. For any polynomial $u \in \mathbf{Z}_S[x_1, ..., x_n]$ monic in x_1 we denote by $q_u, r_u : \mathcal{A} \to \mathcal{A}$ the maps induced by taking the quotient and the

remainder in the division by u. It is an easy consequence of the Composition axiom and the Euclidean division axiom above that if $(f_p) \in \mathcal{F}$, then $(q_u(f_p)), (r_u(f_p)) \in \mathcal{F}$. (A similar statement holds with u monic in any other variable.) Indeed the Euclidean division axiom says our claim is true for the "generic case" when all coefficients of u except the top one are indeterminates; then one specializes using the composition axiom.

Remark 2.15. Let $\phi : \mathcal{A}(m) \to \mathcal{A}(2m)$ be the ring homomorphism such that $\phi(x_k) = (x_k^p + px_{k+m})$ for all $k = 1, ..., m$. By the Composition axiom and Remark 2.11, $\phi(\mathcal{F}) \subset \mathcal{F}$. We claim that for any n

$$\left(\frac{\phi^n(x_1) - x_1^{p^n}}{p} \right) \in \mathcal{F}.$$

For $n = 1$ this is trivial. In general we apply induction; if we apply ϕ to the latter family we get

$$\frac{\phi^{n+1}(x_1) - x_1^{p^{n+1}}}{p} + \frac{x_1^{p^{n+1}} - (x_1^p + px_2)^{p^n}}{p}.$$

So it is enough, by the induction hypothesis and by the Composition axiom, to show that

$$\left(\frac{x_1^{p^n} - (x_1 + px_2)^{p^n}}{p} \right) \in \mathcal{F}.$$

But the latter equals

$$C_{p^n}(x_1, px_2) - p^{p^n - 1} x_2^{p^n}$$

and we are done by Remarks 2.11 and 2.12.

Remark 2.16. Consider the operator

$$\mathbf{Z}[x_1, x_1^{-1}, x_2, ..., x_{n-1}] \to \mathbf{Z}[x_1, x_2, ..., x_{n-1}], \quad h \mapsto h^+,$$
$$\sum_{k=-d}^{m} a_k x_1^k \mapsto \sum_{k=0}^{m} a_k x_1^k$$

(where $a_k \in \mathbf{Z}[x_2, ..., x_{n-1}]$). By continuity we have an induced operator

$$\mathbf{Z}_p[x_1, x_1^{-1}, x_2, ..., x_{n-1}]\hat{}^p \to \mathbf{Z}_p[x_1, x_2, ..., x_{n-1}]\hat{}^p, \quad h \mapsto h^+.$$

We claim that if $(f_p(x_1, x_2, x_3, ..., x_n))$ is Fermat, then $((f_p(x_1^{-1}, x_1, x_2, ..., x_{n-1}))^+)$ is also Fermat. Indeed

$$(f_p(x_1^{-1}, x_1, x_2, ..., x_{n-1}))^+ = (f_p(x_1, x_1^{-1}, x_2, ..., x_{n-1}))^-$$

and we use the Principal part axiom.

Furthermore, assume $(f_p) \in \mathcal{F}(n)$. Then, we claim that for any positive integer μ,

$$(x_n^{p^\mu} f_p(x_1, ..., x_{n-1}, x_n^{-1}))^+$$

belongs to $\mathcal{F}(n)$. Indeed, by the Composition axiom and Remark 2.11 we get

$$(x_2^{p^\mu} f_p(x_3, ..., x_{n+1}, x_1)) \in \mathcal{F}(n+1)$$

and we conclude by applying the remark we just made and, again, the Composition axiom.

Remark 2.17. For any non-negative integer μ let $q_{x_1^{p^\mu}}, r_{x_1^{p^\mu}} : \mathcal{A} \to \mathcal{A}$ be the operators that send a family (f_p) into the family of quotients (respectively remainders) when f_p is divided by $x_1^{p^\mu}$. We claim that these operators map $\mathcal{F}$ into itself. By Remark 2.6 it is enough to check that this is so for the quotient operator $q_{x_1^{p^\mu}}$. But if $(f_p) \in \mathcal{F}(n)$, then, by Remark 2.11, $(x_1^{p^\mu} f_p(x_2, x_3, ..., x_{n+1})) \in \mathcal{F}$. Now we are done by Remark 2.16, noting that

$$q_{x_1^{p^\mu}}(f_p(x_1, ..., x_n)) = (x_1^{-p^\mu} f_p(x_1, ..., x_n))^+ = (g_p(x_1^{-1}, x_1, x_2, ..., x_n))^+,$$

where $g_p(x_1, x_2, x_3, ..., x_{n+1}) := x_1^{p^\mu} f_p(x_2, ..., x_{n+1})$.

In a similar way the corresponding operators $q_{x_k^{p^\mu}}, r_{x_k^{p^\mu}} : \mathcal{A} \to \mathcal{A}$ map $\mathcal{F}$ into $\mathcal{F}$.

We claim now that, for any positive integers n and μ, and for any prime p, one can find polynomials with integer coefficients $A_{1p}, ..., A_{np}$ in the variables $x_1, ..., x_n$ such that the families (A_{1p}),...,(A_{np}) are Fermat, and such that

$$(x_1 + ... + x_n)^{np^\mu} = A_{1p} x_1^{p^\mu} + ... + A_{np} x_n^{p^\mu}.$$

Indeed, by Remark 2.11, $((x_1 + ... + x_n)^{np^\mu})$ is a Fermat family; divide it by $x_1^{p^\mu}$ with a remainder. Call the quotient A_{1p} and divide the remainder by $x_2^{p^\mu}$. Continue in this way; after n divisions one gets a remainder which is homogeneous of degree np^μ and has degree $< p^\mu$ in each of the variables. So this remainder is zero and we are done.

Remark 2.18. We shall repeatedly need the following fact which is a trivial consequence of the $\mathbf{p}-$adic closure axiom and of Remark 2.11: if $2 \in S$, then for any sequence $(a_{2p}), (a_{3p}), ... \in \mathcal{F}(m)$ we have

$$\left(\sum_{n=2}^{\infty} a_{np} \frac{p^{n-2}}{n!} \right) \in \mathcal{F}(m).$$

As one of the (many) applications of this, let $\phi : \mathcal{A}(m) \to \mathcal{A}(2m)$ be as in Remark 2.15. We claim that for any $(f_p) \in \mathcal{F}(m)$ we have

$$\left(\frac{\phi(f_p) - f_p^p}{p} \right) \in \mathcal{F}.$$

Indeed, if u is the $m-$tuple $x_1, ..., x_m$ and y is the $m-$tuple $x_{m+1}, ..., x_{2m}$, the $p-$th component of the above equals

$$\frac{f_p(u^p + py) - f_p(u)^p}{p} = \delta_p f_p + \sum_{|I| \geq 1} \frac{p^{|I|-1}}{|I|!} \frac{|I|!}{I!} \frac{\partial^I f_p}{\partial u^I}(u^p) y^I.$$

Here I are $m-$tuples of natural numbers, $I!$ is the product of the factorials of the components of I, and $|I|$ is the sum of the components of I. We conclude by the Fermat quotient axiom, the Differentiability axiom (Remark 2.10), the Composition axiom, and Remark 2.11.

Remark 2.19. One comment on the operator

$$\delta_{\mathbf{p}} : \mathcal{A}(0) = \prod_{p \notin S} \mathbf{Z}_p \to \prod_{p \notin S} \mathbf{Z}_p, \ (a_p) \mapsto (\delta_p a_p), \ \delta_p a_p = \frac{a_p - a_p^p}{p}$$

considered above is in order. Ihara [16] proposed to see the map

$$d : \mathbf{Z} \to \prod_{p \notin S} \mathbf{F}_p,\ a \mapsto \left(\frac{a - a^p}{p}\ mod\ p \right)$$

as an analogue of diffentiation for integers and he proposed a series of conjectures concerning the "zeroes" of the differential of an integer; these conjectures are completely open. The main difference between Ihara's viewpoint and ours is that we do not consider the reduction mod p of the Fermat quotients but the Fermat quotients themselves. This allows the possibility of iterating our $\delta_{\mathbf{p}}$ which leads to the possibility of considering higher order "differential equations"; and indeed the "differential equations" relevant to our theory will have order two! On the other hand Ihara's operator d cannot be "a priori iterated", at least if we accept a standard conjecture about Mersenne primes. Indeed Voloch proved [26] that if there are infinitely many Mersenne primes, then there is no operator $D : \mathbf{Z} \to \mathbf{Z}$ which, composed with the canonical projection $\mathbf{Z} \to \prod_{p \notin S} \mathbf{F}_p$, yields Ihara's operator d.

Remark 2.20. The analogue, for elliptic curves, of Euler's congruence

$$\left(\frac{a}{p} \right) \equiv a^{\frac{p-1}{2}}\ \ mod\ \ (p) \tag{2.1}$$

is the formula

$$N(p, a, b) \equiv -A_p(a, b)\ \ mod\ \ (p), \tag{2.2}$$

where $N(p, a, b)$ is the number of $\mathbf{F}_p-$points of the affine elliptic curve $y^2 = x^3 + ax + b$ $(a, b \in \mathbf{Z})$ and $A_p(a, b) \in \mathbf{Z}$ is the coefficient of x^{p-1} in $(x^3 + ax + b)^{\frac{p-1}{2}}$. Our main result on elliptic curves should be viewed as a lifting of congruence (2.2) to an equality in characteristic zero in same way in which our formula for the Legendre symbol (1.1) in the Introduction is a lifting of Euler's congruence (2.1) to characteristic zero. Our formula for elliptic curves will be, however, far more complex and far less explicit. Note also that our formula will be "geometric" in the sense that it will hold for a, b integers in an arbitrary finite unramified extension of $\mathbf{Z}_p$.

Remark 2.21. One could try, of course, a naive approach by first expressing $N(p, a, b)$ in Remark 2.20 as

$$N(p, a, b) = p + 1 + \sum_{x=0}^{p-1} \left(\frac{x^3 + ax + b}{p} \right) \tag{2.3}$$

and then expressing $\left(\frac{x^3+ax+b}{p} \right)$ with the help of (1.1) in the Introduction. The resulting expression for $N(p, a, b)$ is not a priori a Fermat adele because, for instance, the summation "symbol" $\sum_{x=0}^{p-1}$ is not allowed in our "Fermat adelic language" and, even "more importantly", because formula (1.1) for $\left(\frac{x^3+ax+b}{p} \right)$ involves denominators which are powers of $x^3 + ax + b$; for each a and b, there will be infinitely many p's such that these denominators will vanish for some x between 0 and $p - 1$. This is something that we do not allow in our theory, and also makes this naive approach "non-geometric".

Remark 2.22. Another naive approach to $N(p,a,b)$ might be based on the formula

$$N(p,a,b) = p + p^{-1}\sum_{t=1}^{p-1}\sum_{x,y=0}^{p-1}\zeta_p^{t(y^2-x^3-ax-b)}, \tag{2.4}$$

where ζ_p is a primitive $p-$th root of unity. The right-hand side of this formula, again, is not a priori a Fermat adele; both the summation symbol and actually ζ_p itself are not part of our "Fermat adelic language", and, again, make this formula "non-geometric".

Remark 2.23. It is interesting to compare our theory with Dwork's [10]; a discussion on this subject is contained in the Appendix to [8]. One aspect, not mentioned in [8], is the following. Dwork's $p-$adic analytic "formula" for the trace of Frobenius of an elliptic curve requires ordinary reduction; so if one keeps an elliptic curve over $\mathbf{Q}$ fixed and one varies p, then Dwork's "formula" only makes sense outside the supersingular primes (which are infinitely many, by Elkies). On the contrary, our "Fermat formula" will make sense for all (but finitely many) p's. This is an interesting contrast between Dwork's theory and ours which deserves being understood. Another interesting contrast is provided by the fact that the Teichmuller lift map appearing in Dwork's formula is a "differential operator of order one" on $\mathbf{Z}_p$ (with respect to δ_p), whereas our "Fermat formula" in Theorem 2.4 below will a priori have order two. On the other hand the Teichmuller lift operator, viewed as a map on the completion of the maximum unramified extension of $\mathbf{Z}_p$, has "infinite order" (it is a "pseudo differential operator") so it will "transcend" the "Fermat paradigm".

Remark 2.24. Here is some preparation for the proof of Theorem 2.6. Let $n \geq 2$ be an integer, and let $(c_p) \in \mathcal{A}(0)$, $(F_p) \in \mathcal{A}(1)$ be defined as follows:

$$c_p = \frac{(p-1)!}{(\frac{p-1}{n})!(p-\frac{p-1}{n})!} \text{ if } p \equiv 1 \mod (n),$$
$$c_p = 0 \text{ if } p \not\equiv 1 \mod (n),$$
$$F_p = c_p x_1^{\frac{p-1}{n}} \text{ if } p \equiv 1 \mod (n),$$
$$F_p = 0 \text{ if } p \not\equiv 1 \mod (n).$$

We claim that (F_p) is Fermat (and, hence, (c_p) is also Fermat, by the Composition axiom). This can be seen as follows. Set

$$c_{p,i} := (-1)^i \frac{(p-1)!}{i!(p-i)!}, \quad 0 < i < p.$$

Then

$$(\sum_{i=1}^{p-1} c_{p,i}(x_2+x_1)^i x_1^{p-i}) \in \mathcal{F}(2).$$

Indeed the latter adele equals

$$(\frac{(x_1-(x_1+x_2))^p - x_1^p + (x_2+x_1)^p}{p}) = (-C_p(x_1,x_2))$$

and the latter is in $\mathcal{F}(2)$ by Remark 2.11. By Remark 2.9 one can divide by x_1 so

$$\left(\sum_{i=1}^{p-1} c_{p,i}(x_2+x_1)^i x_1^{p-1-i}\right) \in \mathcal{F}(2).$$

By the Composition axiom, replacing x_2 by $x_2^{n-1}x_3 - x_1$ we get

$$\left(\sum_{i=1}^{p-1} c_{p,i} x_2^{i(n-1)} x_3^i x_1^{p-1-i}\right) \in \mathcal{F}(3).$$

By Remark 2.16 the adele obtained from the previous adele by substituting $x_1 \mapsto x_1^{-1}$, $x_2 \mapsto x_1$, $x_3 \mapsto x_2$, and dropping the monomials with negative exponents must be in $\mathcal{F}(2)$; in other words

$$\left(\sum_{i \geq \frac{p-1}{n}}^{p-1} c_{p,i} x_1^{in-(p-1)} x_2^i\right) \in \mathcal{F}(2).$$

Now by the Composition axiom we can set $x_1 = 0$ and then replace x_2 by x_1 to get $(F_p) \in \mathcal{F}(1)$.

Proof of Theorem 2.6. Let F_p and c_p be as in Remark 2.24, consider the standard embedding $Y = \mathbf{G}_m \subset \mathbf{A}^2$, $a \mapsto (a, a^{-1})$, let $g = (g_p) = (c_p)$ and let $f = (f_p) \in \mathcal{A}(3)$ be defined by

$$f_p(x_1, x_2, x_3) = F_p(x_1)\left(1 + \sum_{m=1}^{\infty} \{1/n\}_m \frac{p^m}{m!} x_2^{pm} x_3^m\right),$$

where $\{x\}_m := x(x-1)...(x-m+1)$. By Remarks 2.24 and 2.11, we have $f, g \in \mathcal{F}$ and clearly $c_p \in \mathbf{Z}_p^\times$ for all $p \equiv 1 \bmod (n)$. On the other hand, for any $R \in \mathbf{Witt}_p$ and any $P \in R^\times$ with coordinates (a, a^{-1}) the quotient

$$\frac{f_p(a, a^{-1}, \delta a)}{g_p}$$

is $\equiv \bmod (p)$ to $a^{\frac{p-1}{n}}$ and the $n-$power of this quotient clearly equals $\phi(a)/a$. This concludes our proof.

3. Fermat structures: General theory

3.1. A family of ring homomorphisms $(\mathcal{P}(n)^{\wedge p} \to \mathcal{P}(m)^{\wedge p})$, $p \notin S$, will be called *a Fermat family* if the product map $\mathcal{A}(n) \to \mathcal{A}(m)$ maps $\mathcal{F}(n)$ into $\mathcal{F}(m)$. In order for this to happen, it is enough (by the Composition axiom) that the variables $x_1, ..., x_n$ be mapped into $\mathcal{F}(m)$.

Assume we are given a family (A_p) of rings, indexed by $p \notin S$; by *a Fermat structure* on this family we shall understand a family of surjective ring homomorphisms $(\mathcal{P}(n)^{\wedge p} \to A_p)$ (where n does not vary with p). Here $\mathcal{F}$ does not play any role but it is convenient, for simplicity, to still call this structure *Fermat*. If we are given a Fermat structure as above, then an element $(a_p) \in \prod_{p \notin S} A_p$ will be called *a Fermat family* if it lies in the image of

$$\mathcal{F}(n) \subset \mathcal{A}(n) \to \prod_{p \notin S} A_p.$$

Note that the image of the above ring homomorphism is not, a priori, $\mathbf{p}-$adically closed. A family in $\prod_{p \notin S} A_p$ will be called *formally Fermat* if it is a $\mathbf{p}-$adic limit of Fermat families. Assume we are given two families of rings (A_p) and (B_p) each equipped with Fermat structures, say $(\mathcal{P}(n)^{\wedge p} \to A_p)$ and $(\mathcal{P}(m)^{\wedge p} \to B_p)$. A family of ring homomorphisms $(A_p \to B_p)$ will be called *Fermat* (with respect to our Fermat structures) if it is induced by a Fermat family of homomorphisms $(\mathcal{P}(n)^{\wedge p} \to$

$\mathcal{P}(m)^{\wedge p}$). (An important remark is here in order: if $(A_p \to B_p)$ is Fermat, and, for each p, $A_p \to B_p$ is an isomorphism, it does not follow a priori that the family of the inverses $(B_p \to A_p)$ is Fermat.) Let $\mathcal{F}\mathbf{Alg}$ denote the category whose objects are families of rings (A_p) equipped with a Fermat structure and whose morphisms $(A_p) \to (B_p)$ are the Fermat families $(A_p \to B_p)$ of homomorphisms. Note that if (A_p), (B_p) and (C_p) have Fermat structures $(\mathcal{P}(n)^{\wedge p} \to A_p)$, $(\mathcal{P}(m)^{\wedge p} \to B_p)$, and $(\mathcal{P}(r)^{\wedge p} \to C_p)$ respectively, and if $(C_p \to A_p)$, $(C_p \to B_p)$ are Fermat families of homomorphisms, then $(A_p \hat{\otimes}_{C_p} B_p)$ has a naturally induced Fermat structure $(\mathcal{P}(m+n)^{\wedge p} \to A_p \hat{\otimes}_{C_p} B_p)$ called the *product Fermat structure*. Also if $(A_p \to A'_p)$, $(B_p \to B'_p)$, and $(C_p \to C'_p)$ are Fermat families, so is $(A_p \hat{\otimes}_{C_p} B_p \to A'_p \hat{\otimes}_{C'_p} B'_p)$. A (trivial) example of objects of $\mathcal{F}\mathbf{Alg}$ is the following. Let $\mathbf{Alg}$ denote the category of finitely generated $\mathbf{Z}_S-$algebras. If A is an object of $\mathbf{Alg}$ and $p \notin S$, then we denote by $A^{\wedge p}$ the $p-$adic completion of A. For any A as above consider the family $(A^{\wedge p})$. Any surjective homomorphism $\pi : \mathbf{Z}_S[x_1, ..., x_n] \to A$ induces, by passing to $p-$adic completions, a Fermat structure on $(A^{\wedge p})$ hence an object of $\mathcal{F}\mathbf{Alg}$. Such a Fermat structure will be called *standard*. If we replace π by another surjection, then we obtain another object of $\mathcal{F}\mathbf{Alg}$, isomorphic in $\mathcal{F}\mathbf{Alg}$ to the first one. (Note that if an element $(a_p) \in \prod_{p \notin S} A^{\wedge p}$ is a Fermat family with respect to a standard Fermat structure, it is a Fermat family with respect to any other standard Fermat structure.) On the other hand if we fix, for each A in $\mathbf{Alg}$, a surjection π as above, then we get a functor $\mathbf{Alg} \to \mathcal{F}\mathbf{Alg}$.

Non-trivial examples will appear when we consider $p-$jet spaces in the next section.

In what follows we want to globalize the above notions. One could do this in a "ringed space theoretic style" but this would introduce unnecessary complications; we prefer to present the theory in a more ad hoc manner, for this is enough for all applications we have in mind and is definitely more economical.

3.2. In what follows a formal scheme over $\mathbf{Z}_p$ will always mean a formal scheme locally isomorphic to the $p-$adic completion of a scheme of finite type over $\mathbf{Z}_p$. Let (X_p) be a family indexed by $p \notin S$, where each X_p is a formal scheme over $\mathbf{Z}_p$. Giving *a Fermat structure* on (X_p) will mean, by definition, that:

1) One is given a partially ordered set $(I, \leq)$.

2) For each $p \notin S$ one is given an affine open covering $(X_p^{(i)})_{i \in I}$ of X_p, such that $X_p^{(i)} \subset X_p^{(j)}$ whenever $i \leq j$.

3) For each $i \in I$ one is given a Fermat structure on the family $(\mathcal{O}(X_p^{(i)}))$, such that for all $i \leq j$ the family of restriction maps $(\mathcal{O}(X_p^{(j)}) \to \mathcal{O}(X_p^{(i)}))$ is Fermat (i.e. it is a morphism in $\mathcal{F}\mathbf{Alg}$).

By abuse, we shall say that $((X_p^{(i)})_{i \in I})$ is a Fermat structure on (X_p).

If I consists of one element only we say the Fermat structure is *coarse*. A coarse structure can only exist, of course, if all the X_p's are affine.

Assume now we are given two families of formal schemes (X_p) and (Y_p) with Fermat structures $((X_p^{(i)})_{i \in I})$ and $((Y_p^{(j)})_{j \in J})$, respectively. Let

$$(\pi_p : X_p \to Y_p)$$

be a family of morphisms of formal schemes. We say that this family is *a Fermat family* if for any $j \in J$ there exists a subset $I(j) \subset I$ with the property that for all

p we have

$$\pi_p^{-1}(Y_p^{(j)}) = \bigcup_{i \in I(j)} X_p^{(i)}$$

and for all $i \in I(j)$ the induced family of maps

$$(\mathcal{O}(Y_p^{(j)}) \to \mathcal{O}(X_p^{(i)}))$$

is Fermat (i.e. it is a morphism in $\mathcal{F}\mathbf{Alg}$). A composition of two Fermat families of morphisms is Fermat. We shall denote by $\mathcal{F}\mathbf{Sch}$ the category whose objects are families (X_p) of formal schemes with Fermat structures and whose morphisms $(X_p) \to (Y_p)$ are Fermat families $(X_p \to Y_p)$ of morphisms.

Here are some (trivial but useful) examples/definitions. Non-trivial examples will appear when we consider $p-$jet spaces in the next section.

First, let $\mathcal{F}\mathbf{Sch}_{coarse}$ be the full subcategory of $\mathcal{F}\mathbf{Sch}$ whose objects are those with coarse Fermat structure. Then there is a functor $\mathcal{F}\mathbf{Alg} \to \mathcal{F}\mathbf{Sch}_{coarse}$; it associates to any object (A_p) in $\mathcal{F}\mathbf{Alg}$ the family $(Spf\ A_p)$ with the coarse Fermat structure.

Another example can be constructed as follows. Let $\mathbf{Sch}$ denote the category of schemes of finite type over $\mathbf{Z}_S$. Let X be an object of $\mathbf{Sch}$. On the family $(X^{\wedge p})$ of the $p-$adic completions of X one can put the following Fermat structure called the *full* Fermat structure. We take the index set I to be in bijection with the set of all affine open subsets of X (for $i \in I$ we denote by $X_i \subset X$ the corresponding open set), we let $i \leq j$ iff $X_i \subset X_j$, we set $X_p^{(i)} := {X_i}^{\wedge p}$, we **choose** isomorphisms $\sigma_i : \mathbf{Z}_S[T]/(f) \simeq \mathcal{O}(X_i)$ (where T is a tuple of indeterminates and f is a tuple of polynomials), and we put on $(\mathcal{O}({X_i}^{\wedge p})) = (\mathcal{O}(X_i)^{\wedge p})$ the standard Fermat structure defined by the surjection $\mathbf{Z}_S[T] \to \mathcal{O}(X_i)$. In this way $(X^{\wedge p})$ becomes an object $(X_p)_{full}$ in $\mathcal{F}\mathbf{Sch}$. If we change the collection of isomorphisms (σ_i) the new object of $\mathcal{F}\mathbf{Sch}$ will be isomorphic to the original one. On the other hand, if for any X we fix such a collection (σ_i), then we obtain a functor $\mathbf{Sch} \to \mathcal{F}\mathbf{Sch}$.

(N.B. We have previously defined a functor $\mathbf{Alg} \to \mathcal{F}\mathbf{Alg}$ and we also have an obvious functor $\mathbf{Alg} \to \mathbf{Sch}$; note however that the functor $\mathbf{Alg} \to \mathcal{F}\mathbf{Alg} \to \mathcal{F}\mathbf{Sch}_{coarse} \to \mathcal{F}\mathbf{Sch}$ is not isomorphic to $\mathbf{Alg} \to \mathbf{Sch} \to \mathcal{F}\mathbf{Sch}$.)

Finally, another more general example that will play a role later is obtained by considering an affine morphism of $\mathbf{Z}_S-$schemes of finite type $\pi : X \to Y$; put on $(X^{\wedge p})$ the Fermat structure whose index set is the set J of all affine open sets Y_j of Y and whose open sets are $X_p^{(j)} := \pi^{-1}(Y_j)^{\wedge p}$, with standard Fermat structure on $(\mathcal{O}(\pi^{-1}(Y_j)^{\wedge p}))$. We get an object of $\mathcal{F}\mathbf{Sch}$ denoted by $(X^{\wedge p})_{ind}$ whose Fermat structure we call *induced from* Y via π.

3.3. Let (Y_p) be an object of $\mathcal{F}\mathbf{Sch}$, i.e. a family of formal schemes equipped with a Fermat structure $((Y_p^{(j)})_{j \in J})$; moreover, for each j, let $(\mathcal{P}(n_j)^{\wedge p} \to \mathcal{O}(Y_p^{(j)}))$ be the defining Fermat structure on $(\mathcal{O}(Y_p^{(j)}))$. Now let (X_p) be a family of formal schemes. We say that (X_p) is *closed* in (Y_p) if each X_p is a closed formal subscheme of Y_p. If this is the case, then we can define the *deduced* Fermat structure on (X_p) by taking the same index set J and setting $X_p^{(j)} := Y_p^{(j)} \cap X_p$ with Fermat structure on $(\mathcal{O}(Y_p^{(j)} \cap X_p))$ defined by the surjections $\mathcal{P}(n_j)^{\wedge p} \to \mathcal{O}(Y_p^{(j)}) \to \mathcal{O}(Y_p^{(j)} \cap X_p)$. Clearly, the family of embeddings $(X_p \to Y_p)$ is Fermat.

Proposition 3.1. *Assume that (Z_p) and (Y_p) are objects of $\mathcal{F}\mathbf{Sch}$ and $(Z_p \to Y_p)$ is a morphism in $\mathcal{F}\mathbf{Sch}$. Assume (X_p) is closed in (Y_p) and view (X_p) with its deduced Fermat structure. Assume that for each p the morphism of formal schemes $Z_p \to Y_p$ factors through a morphism of formal schemes $Z_p \to X_p$. Then $(Z_p \to X_p)$ is a Fermat family.*

Proof. A trivial exercise. □

The next proposition deals with the "local character" of Fermat families.

Proposition 3.2. *Let U be an integral affine scheme of finite type over Spec $\mathbf{Z}_S$, with integral fibers, and dominating Spec $\mathbf{Z}_S$, and let (U_i) be an affine open covering of U. Then there exists a finite set of places S' containing S satisfying the following property: if a family*

$$(a_p) \in \prod_{p \notin S} \mathcal{O}(U^{\wedge p})$$

is such that for each i the image of (a_p) in $\prod_{p \notin S} \mathcal{O}(U_i{}^{\wedge p})$ is a formally Fermat family, then the image of (a_p) in $\prod_{p \notin S'} \mathcal{O}(U^{\wedge p})$ is formally Fermat.

(Here $(\mathcal{O}(U_i{}^{\wedge p}))$ and $(\mathcal{O}(U^{\wedge p}))$ are viewed with their standard Fermat structure.) We stress the fact that S' depends only on U and U_i and not on (a_p). It is not clear if in the above proposition we may replace "formally Fermat" by "Fermat".

To prove Proposition 3.2 we need the following lemma in commutative algebra:

Lemma 3.3. *Let A be an integral domain, let $p \in A$ be a prime element, let $I \subset A$ be a prime ideal, not containing p, such that (I, p) is also prime, and let $g \in A$, $g \notin (I, p)$. Then, for any positive integer n, the map $A/p^n A \to (A/p^n A)_g$ is injective and*

$$I(A/p^n A)_g \cap (A/p^n A) = I(A/p^n A).$$

Proof. The injectivity of $A/p^n A \to (A/p^n A)_g$ is trivial. Now assume $a \in A$ is such that its image in $A/p^n A$ belongs to $I(A/p^n A)_g \cap (A/p^n A)$ and let us prove that the image of a in $A/p^n A$ lies in $I(A/p^n A)$. One can write

$$ag^k = b + p^n c$$

with $b \in I$, $c \in A$, $k \geq 0$. In particular $ag^k \in (I, p)$. Hence $a \in (I, p)$. Write

$$a = d + pa_1,$$

$d \in I$, $a_1 \in A$. We get $pa_1 g^k = (b - dg^k) + p^n c$. It follows that p divides $b - dg^k$ which is in I. Since I is prime and does not contain p we have $b - dg^k = pb_1$ with $b_1 \in I$. Dividing by p we get

$$a_1 g^k = b_1 + p^{n-1} c.$$

Now we can repeat the argument and find a sequence $a_2, ..., a_n$ such that

$$a_1 = d_1 + pa_2, ..., a_{n-1} = d_{n-1} + pa_n, \quad d_1, ..., d_{n-1} \in I.$$

Hence we compute

$$a = d + pd_1 + p^2 d_2 + ... + p^{n-1} d_{n-1} + p^n a_n \in (I, p^n)$$

which closes the proof. □

Proof of Proposition 3.2. Write $U = Spec\ \mathbf{Z}_S[x]/I$, x a tuple of indeterminates; then I is prime and for each $p \notin S$, we have $p \notin I\mathbf{Z}_{(p)}[x]$, and $(I,p)\mathbf{Z}_{(p)}[x]$ is prime. Cover each U_i by affine open sets W which are principal in U; since the image of (a_p) in $\prod_{p\notin S}\mathcal{O}(W^{\wedge p})$ will be a formally Fermat family, we may assume that our covering (U_i) is finite ($i \in \{1,...,m\}$) and all U_i are principal in U. So we can write $U_i = Spec\ (\mathbf{Z}_S[x]/I)_{g_i} = \mathbf{Z}_S[x,y_i]/(I, g_iy_i - 1)$, where $g_1,...,g_m \in \mathbf{Z}_S[x]$ are such that $h_1g_1 + ... + h_mg_m = 1 - b$ with $h_i \in \mathbf{Z}_S[x]$, $b \in I$. Set $g = g_1...g_m \in \mathbf{Z}_S[x]$. Let S' be a finite set of primes such that $g \notin (I,p)\mathbf{Z}_{(p)}[x]$ for all $p \notin S'$. At this point we may replace S by S'.

Let a_p be the image of some $F_p = F_p(x) \in \mathbf{Z}_p[x]^{\wedge p}$ and fix a positive integer ν. By hypothesis there exist $F_{ip}, K_{ip} \in \mathbf{Z}_p[x,y_i]^{\wedge p}$ such that (F_{ip}) is a Fermat family for each i and such that

$$F_p(x) - F_{ip}(x,y_i) = \sum_j b_{ij}c_{ij} + (g_iy_i - 1)c_i + p^\nu K_{ip}(x,y_i) \tag{3.1}$$

in the ring $\mathbf{Z}_p[x,y_i]^{\wedge p}$, where $b_{ij} \in I$, $c_{ij}, c_i \in \mathbf{Z}_p[x,y_i]^{\wedge p}$. Set $y_i \mapsto 1/g_i \in (\mathbf{Z}_p[x]_g)^{\wedge p}$ in equation (3.1); we get an equality in the ring $(\mathbf{Z}_p[x]_g)^{\wedge p}$

$$F_p(x) - F_{ip}(x,g_i^{-1}) = \sum_j b_{ij}\tilde{c}_{ij} + p^\nu K_{ip}(x,g_i^{-1}), \tag{3.2}$$

where $\tilde{c}_{ij} \in (\mathbf{Z}_p[x]_g)^{\wedge p}$. By Remark 2.8 there exists a positive integer μ such that each F_{ip} is congruent modulo p^ν to a polynomial in $\mathbf{Z}_p[x,y_i]$ of degree $\le p^\mu$. Hence we can write, in the ring $\mathbf{Z}_p[x,z,z^{-1}]^{\wedge p}$ (where z is a variable),

$$z^{p^\mu}F_{ip}(x,z^{-1}) = z^{p^\mu}\Phi_{ip}^{(\nu)}(x,z^{-1}) + p^\nu\Psi_{ip}^{(\nu)}, \tag{3.3}$$

where $\Phi_{ip}^{(\nu)}$ is a polynomial of degree $\le p^\mu$ in $\mathbf{Z}_p[x,z]$ and $\Psi_{ip}^{(\nu)} \in \mathbf{Z}_p[x,z,z^{-1}]^{\wedge p}$. Applying the operator $f \mapsto f^+$ "with respect to z" (cf. Remark 2.16) to equation (3.3) we get

$$(z^{p^\mu}F_{ip}(x,z^{-1}))^+ = z^{p^\mu}\Phi_{ip}^{(\nu)}(x,z^{-1}) + p^\nu(\Psi_{ip}^{(\nu)})^+. \tag{3.4}$$

Set $\tilde{F}_{ip}^{(\nu)} := (z^{p^\mu}F_{ip}(x,z^{-1}))^+$; by Remark 2.16 $(\tilde{F}_{ip}^{(\nu)})$ is a Fermat family. Subtracting equation (3.4) from equation (3.3) we get

$$z^{p^\mu}F_{ip}(x,z^{-1}) = \tilde{F}_{ip}^{(\nu)} + p^\nu\tilde{\Psi}_{ip}^{(\nu)}, \tag{3.5}$$

where $\tilde{\Psi}_{ip}^{(\nu)} \in \mathbf{Z}_p[x,z,z^{-1}]^{\wedge p}$. Setting $z \mapsto g_i$ in the last equality we get an equation

$$g_i^{p^\mu}F_{ip}(x,g_i^{-1}) = F_{ip}^{(\nu)} + p^\nu\Psi_{ip}^{(\nu)} \tag{3.6}$$

in the ring $(\mathbf{Z}_p[x]_g)^{\wedge p}$, where $F_{ip}^{(\nu)} \in \mathbf{Z}_p[x]^{\wedge p}$, $(F_{ip}^{(\nu)})$ is a Fermat family (by the Composition axiom), and $\Psi_{ip}^{(\nu)} \in (\mathbf{Z}_p[x]_g)^{\wedge p}$. Combining equations (3.1) and (3.6) we get

$$g_i^{p^\mu}F_p = F_{ip}^{(\nu)} + p^\nu\Theta_{ip}^{(\nu)} + \sum_j b_{ij}c_{ij}^{(\nu)}, \tag{3.7}$$

where $c_{ij}^{(\nu)}, \Theta_{ip}^{(\nu)} \in (\mathbf{Z}_p[x]_g)^{\wedge p}$. Let $A_{1p},...,A_{np}$ be as in the Remark 2.17. In particular they are polynomials in n variables with integer coefficients, they form Fermat

families, and

$$(1-b)^{np^\mu} = (\sum_{i=1}^{n} h_i g_i)^{np^\mu} = \sum_{i=1}^{n} H_{ip} g_i^{p^\mu}, \tag{3.8}$$

where $H_{ip} := A_{ip}(h_1 g_1, ..., h_n g_n) h_i^{p^\mu} \in \mathbf{Z}_{(p)}[x]$. Clearly, (H_{ip}) are Fermat families. Multiplying equation (3.7) by H_{ip} and taking the sum over all i we get

$$F_p = F_p^{(\nu)} + p^\nu \Theta_p^{(\nu)} + \sum_j b_j c_j^{(\nu)}, \tag{3.9}$$

where $F_p^{(\nu)} \in \mathbf{Z}_p[x]^{\wedge p}$ form a Fermat family, $\Theta_p^{(\nu)} \in (\mathbf{Z}_p[x]_g)^{\wedge p}$, $b_j \in I$, and $c_j^{(\nu)} \in (\mathbf{Z}_p[x]_g)^{\wedge p}$. Consider the image of equation (3.9) via the surjection

$$(\mathbf{Z}_p[x]_g)^{\wedge p} \to (\mathbf{Z}_p[x]_g)^{\wedge p}/(p^\nu) = \left(\frac{\mathbf{Z}_{(p)}[x]}{p^\nu \mathbf{Z}_{(p)}[x]}\right)_g$$

and denote by $\bar{F}_p$ and $\bar{F}_p^{(\nu)}$ the images of F_p and $F_p^{(\nu)}$ via this surjection. By Lemma 3.3 applied to $A = \mathbf{Z}_{(p)}[x]$ we have

$$\frac{\mathbf{Z}_{(p)}[x]}{p^\nu \mathbf{Z}_{(p)}[x]} \subset \left(\frac{\mathbf{Z}_{(p)}[x]}{p^\nu \mathbf{Z}_{(p)}[x]}\right)_g,$$

$$\bar{F}_p - \bar{F}_p^{(\nu)} \in I\left(\frac{\mathbf{Z}_{(p)}[x]}{p^\nu \mathbf{Z}_{(p)}[x]}\right)_g \cap \left(\frac{\mathbf{Z}_{(p)}[x]}{p^\nu \mathbf{Z}_{(p)}[x]}\right) = I\left(\frac{\mathbf{Z}_{(p)}[x]}{p^\nu \mathbf{Z}_{(p)}[x]}\right).$$

Consequently

$$F_p - F_p^{(\nu)} \in I\mathbf{Z}_p[x]^{\wedge p} + p^\nu \mathbf{Z}_p[x]^{\wedge p}$$

and we are done since the image $a_p^{(\nu)}$ of $F_p^{(\nu)}$ in $\mathcal{O}(U^{\wedge p})$ is congruent modulo p^ν to a_p.

Proposition 3.4. *Let $u \in \mathbf{Z}_S[x_1, ..., x_n]$ be a polynomial and let*

$$U = Spec\ \mathbf{Z}_S[x_1, ..., x_n]/(u)$$

be the "hypersurface defined by u". Then there exists a finite set of primes S', containing S, such that any formally Fermat family in $\prod_{p \notin S'} \mathcal{O}(U^{\wedge p})$ is Fermat.

Proof. After a linear change of variables and after enlarging S to some S' we may assume u is monic in x_n. Now let $(f_p) \in \prod_{p \notin S'} \mathcal{O}(U^{\wedge p})$ be a $\mathbf{p}-$adic limit of Fermat families $(f_p^{(\nu)})$ in this ring. Let $(F_p), (F_p^{(\nu)}) \in \prod_{p \notin S'} \mathcal{P}(n)^{\wedge p}$ be liftings of $(f_p), (f_p^{(\nu)})$ with $(F_p^{(\nu)})$ Fermat. We may write

$$F_p = F_p^{(\nu)} + p^\nu H_p^{(\nu)} + u G_p^{(\nu)}$$

for some $H_p^{(\nu)}, G_p^{(\nu)} \in \mathcal{P}(n)^{\wedge p}$. To conclude apply, to the above equality, the endomorphism r_u of $\mathcal{P}(n)^{\wedge p}$ that takes the remainder when a series is divided by u. By Remark 2.14 we get that $(r_u(F_p))$ is Fermat, hence (f_p) is Fermat. □

Next we will be concerned with residues of "Fermat" families of $1-$forms. We need some preparation.

3.4. Let M be a Noetherian ring and let C/M be a curve (by which we will mean here a smooth projective morphism $C \to B = Spec\ M$, of relative dimension one, with connected fibers). Let $\Gamma \subset C$ be a closed subscheme in C, and let $V \subset C$ be an affine open subset containing Γ. Then V will be called a *prepared* neighborhood of Γ if it has the form $V = Spec((M[x,y]/(g))_h)$, where $g \in M[x,y]$, $h \in M[x]$, such that, upon denoting $W := Spec(M[x]_h)$, the following conditions are satisfied:

1. g is monic in y (in particular V is finite over W), and
2. V is etale over W.

If $\Gamma = P$ above is the image of an $M-$point $P \in C(M)$ and if $O \in W(M)$ denotes the $M-$point of W defined by $x \mapsto 0$, we may, and will, assume that, in the definition above, $P \mapsto O$ via $V(M) \to W(M)$ and $h(0) = 1$; indeed, if $P \mapsto O$, then $h(0)$ is automatically invertible in M.

Lemma 3.5. *Let C/M be a curve, where $M = k$ is a field of characteristic zero, let $\Gamma \subset C$ be a closed subscheme, and let $U \subset C$ be an affine neighborhood of Γ in C. Then there exists a prepared neighborhood V of Γ contained in U.*

Proof. This is a simple fact of projective geometry. Embed k into an algebraic closure $\bar{k}$ of k and replace all schemes with their sets of $\bar{k}-$rational points. Set $T = C \backslash U$. Embed C into a projective space and let $\pi : C \to C' \subset \mathbf{P}^2$ be a succession of projections with centers $k-$rational points. Let T' be the union of $\pi(T)$ with the singular locus of C'. Then, upon choosing the projection points suitably, we may assume that for any $P \in \Gamma$ we have $P' := \pi(P) \notin T'$ and $C \to C'$ is birational. Choose projective coordinates X, Y, Z in $\mathbf{P}^2$, defined over k, such that, denoting by L_X, L_Y, L_Z the lines defined by the vanishing of the corresponding coordinates, we have $\pi(\Gamma) \cap L_Z = \emptyset$. Consider the affine coordinates $x = X/Z$, $y = Y/Z$, and let $g(x,y) = 0$ be the affine equation of C' in these coordinates, with g having coefficients in k. For $\lambda \in k$ set $X_1 = X - \lambda Y$, $x_1 = x - \lambda y$. Then we can write

$$g(x,y) = g(x_1 + \lambda y, y) = g_1(x_1, y)$$

where $g_1 \in k[x_1, y]$. Consider the projection $\varphi_{P'} : C' \to L_Z$ of center P' and let $Q_\lambda = (\lambda : 1 : 0)$. Also, for any morphism f between (possibly singular) curves denote by $Ram(f)$ the set of all $\bar{k}-$rational points in the source curve where f is not etale. Then for all except finitely many values of λ the following conditions hold:

1) The polynomial g_1 is monic in y,
2) $Ram(\varphi) \cap \varphi_{P'}^{-1}(Q_\lambda) = \emptyset$, for any $P \in \Gamma$,
3) Q_λ is not on the tangent to C' at the point P', for any $P \in \Gamma$,
4) Q_λ is not on any of the lines $P'Q'$ for any $P \in \Gamma$, $Q' \in T'$ and
5) Q_λ is not on C'.

Now consider the projection $\psi : C' \to L_Y$ of center Q_λ. The above properties imply that:

a) $\psi^{-1}(\psi(P')) \cap T' = \emptyset$ for any $P \in \Gamma$, and
b) $Ram(\psi) \cap \psi^{-1}(\psi(P')) = \emptyset$ for any $P \in \Gamma$.

Define the following sets:

$$T'' = \psi(Ram(\psi) \cup T') \cup \{(1:0:0)\} \subset L_Y,$$
$$W = L_Y \backslash T'',$$
$$V' = C' \backslash \psi^{-1}(T'') \subset C',$$
$$V = \pi^{-1}(V').$$

Note that the morphism $V' \to W$ is finite and etale, while $V \to V'$ is an isomorphism (because V' is non-singular). Finally note that $\Gamma \subset V \subset U$. Now ψ is given in projective coordinates by $(X, Y, Z) \mapsto (X - \lambda Y, Z)$ hence, in affine coordinates by $(x, y) \mapsto x - \lambda y = x_1$. Therefore $V \simeq V' \to W$ is given by taking the tensor product with $\bar{k}$ of an inclusion of rings $k[x_1]_h \to (k[x_1, y]/(g_1))_h$, where $h \in k[x_1]$ is the polynomial whose roots in $\bar{k}$ are the x_1-coordinates of the points in T''. □

Corollary 3.6. *Let C/M be a curve, let $\Gamma \subset C$ be a closed subscheme, and let U be an affine neighborhood of Γ in C. Assume M is an integral domain of characteristic zero. Then, after replacing Spec M by a Zariski open set of it, one can find a prepared neighborhood of Γ contained in U.*

3.5. Let C/B be a curve, $B = Spec\ M$, let $P \in C(M)$ be an $M-$point on it, assume V is a prepared neighborhood of P and assume M is an integral domain of characteristic zero. Let $\omega \in H^0(V, \Omega_{C/B})$ and $\eta \in \mathcal{O}(V \backslash P)$. Consider $Res_P(\eta\omega)$, the residue of $\eta\omega$ at P, which is a priori an element of the fraction field of M. It will be important later to compute this residue as follows. Let $V = Spec((M[x, y]/(g))_h)$ and $W := Spec(M[x]_h)$ be as in Section 3.4 above; hence $V \backslash P = Spec((M[x, y]/(g))_{xh})$. Assume η is given as the image, modulo g, of an element $f \in (M[x]_{xh})[y]$. Since g is monic (say, of degree d) in y we can consider the remainder $r_g(f)$ when f is divided by g and write it in the form

$$r_g(f) = f_0 + f_1 y + ... + f_{d-1} y^{d-1},$$

where $f_i \in M[x]_{xh}$. Since $V \to W$ is etale we may write $\omega = udx$, where $u \in M[x]_h$. Let $Tr : (M[x, y]/(g))_{xh} \to M[x]_{xh}$ be the trace map. Then

$$Tr(\eta\omega) = Tr(u \sum_{i=0}^{d-1} f_i y^i dx) = (u \sum_{i=0}^{d-1} f_i Tr(y^i))dx \in M[x]_{xh} dx \subset M((x))dx.$$

The coefficient of $x^{-1}dx$ in the above expression equals the usual residue $Res_O(Tr(\eta\omega))$. Since $\psi : V \to W$ is finite, by [23], p. 22, we have

$$Res_O(Tr(\eta\omega)) = \sum_{\psi(Q)=O} Res_Q(\eta\omega),$$

where Q runs through the set of all $\bar{k}-$points of V mapped to O by ψ, where $\bar{k}$ is the algebraic closure of the fraction field k of M. However, since $\eta\omega$ is regular on $V \backslash P$, the right-hand side of the above equality reduces to $Res_P(\eta\omega)$. Consequently $Res_P(\eta\omega)$ is simply the coefficient of x^{-1} in the sum

$$u \sum_{i=0}^{d-1} f_i Tr(y^i) \in M[x]_{xh}.$$

Note in particular that $Res_P(\eta\omega)$ belongs to M (and not merely to k).

The above discussion generalizes, in an obvious way, to the case when M is a product of integral domains (rather than an integral domain). This is the case, for instance, when M is a smooth $\mathbf{Z}-$algebra or some $p-$adic completion of a smooth $\mathbf{Z}-$algebra.

The construction above allows one to define $Res_P(\hat{\eta}\omega) \in M^{\hat{}p}$ for any $\hat{\eta} \in \mathcal{O}(V\backslash P)^{\hat{}p}$. (Here $\hat{}p$ denotes, as usual, the $p-$adic completion, and note that such an $\hat{\eta}$ can have an "essential singularity" at P.) Indeed one takes a sequence $\eta^{(\nu)} \in \mathcal{O}(V\backslash P)$ converging $p-$adically to $\hat{\eta}$ and one defines $Res_P(\hat{\eta}\omega)$ as the $p-$adic limit of the $Res_P(\eta^{(\nu)}\omega)$'s. This definition is, of course, independent of the choice of V.

Lemma 3.7. *Assume M is a smooth $\mathbf{Z}-$algebra, S is a finite set of primes, C/M is a curve, $P \in C(M)$ is a point, V is a prepared neighborhood of P in C, $\omega \in H^0(V, \Omega_{C/M})$ is a regular $1-$form on V and*

$$(\hat{\eta}_p) \in \prod_{p \notin S} \mathcal{O}(V\backslash P)^{\hat{}p}$$

is a formally Fermat family outside S (with respect to the standard structure). Then the family of residues

$$Res_P(\hat{\eta}_p\omega) \in \prod_{p \notin S} M^{\hat{}p}$$

is formally Fermat outside S.

Proof. Represent M as $\mathbf{Z}[t]/(v)$, where t is a tuple of indeterminates and v is a tuple of polynomials. Also, let us borrow our notations from Section 3.5 above. By hypothesis there exists a sequence of Fermat families

$$(F_p^{(\nu)}) \in \prod_{p \notin S} \mathbf{Z}_p[t, x, y, z]^{\hat{}p}$$

whose image in $\prod_{p \notin S} \mathcal{O}(V\backslash P)^{\hat{}p}$ (via the map $z \mapsto (xh)^{-1}$) converges $\mathbf{p}-$adically to (η_p). Let $\hat{\eta}_p^{(\nu)} \in \mathcal{O}(V\backslash P)^{\hat{}p}$ be the image of $F_p^{(\nu)}$. Let $r_g : \mathbf{Z}_p[t, x, y, z]^{\hat{}p} \to \mathbf{Z}_p[t, x, y, z]^{\hat{}p}$ be the operator that takes the remainder in the division by g (where polynomials are viewed in the variable y). By Remark 2.14, the family $(r_g(F_p^{(\nu)}))$ is Fermat. Write

$$r_g(F_p^{(\nu)}) = \sum_{i=0}^{d-1} F_{ip}^{(\nu)} y^i,$$

where $F_{ip}^{(\nu)} \in \mathbf{Z}_p[t, x, z]^{\hat{}p}$. By Remark 2.9, the families $(F_{ip}^{(\nu)})$ are Fermat. Write $\omega = udx$, with u the image of some $U \in \mathbf{Z}[t, x, w]$ via $w \mapsto h^{-1}$. Also let $Tr(y^i) \in M[x]_h$ be images of $\Theta_i \in \mathbf{Z}[t, x, w]$. Then, for each ν, the family

$$(G_p^{(\nu)}(t, x, z, w)) := (U(t, x, w) \sum_{i=0}^{d-1} F_{ip}^{(\nu)}(t, x, z)\Theta_i) \in \prod_{p \notin S} \mathbf{Z}_p[t, x, z, w]^{\hat{}p}$$

is Fermat. Let $H \in \mathbf{Z}[t, x]$ be a lifting of h with $H(t, 0) = 1$. Then, by Remarks 2.9 and 2.13, the coefficient of x^{-1} in $(G_p^{(\nu)}(t, x, (xH)^{-1}, H^{-1}))$ is a Fermat family in $\prod_{p \notin S} \mathbf{Z}_p[t]^{\hat{}p}$. By Section 3.5 above the latter family projects into $(Res_P(\hat{\eta}_p^{(\nu)}\omega)) \in \prod_{p \notin S} M^{\hat{}p}$, hence this latter family is Fermat. It follows that $(Res_P(\hat{\eta}_p\omega)) \in \prod_{p \notin S} M^{\hat{}p}$ is formally Fermat and our lemma is proved. □

3.6. Let M be a Noetherian ring, let C/M be a curve, and let $\mathcal{U} = (U_i)_{i\in I}$ be an affine open covering. We say that $\mathcal{U}$ is *prepared* if:

1) For each $i \in I$ the open set $C\backslash U_i$ is the union of the images of a finite set $Z_i \subset C(M)$ of $M-$points of C and the points in $Z := \bigcup Z_i$ are disjoint.

2) For any $P \in Z$ there exists a prepared neighborhood V_P of P contained in $(C\backslash Z) \cup \{P\}$.

In 1) above by the points of Z being disjoint we mean, of course, that the images of the corresponding maps $Spec\ M \to C$ are disjoint. This being the case, $(C\backslash Z)\cup\{P\} = C\backslash(Z\backslash\{P\})$ is then an open set containing P. Corollary 3.6 implies the following:

Corollary 3.8. *Let C/M be a curve where M is an integral domain of characteristic zero, and let $\mathcal{U}$ be an affine open covering of C. Then, after replacing Spec M by a dense etale open set of it, $\mathcal{U}$ becomes prepared.*

3.7. Let M be a smooth $\mathbf{Z}-$algebra, let C/M be a curve, let $\mathcal{U}$ be an affine open covering of C, and let $\omega \in H^1(C, \Omega_{C/M})$ be a global $1-$form. We need to review the construction of the map

$$\langle\ ,\omega\rangle : H^1(C \otimes M^{\wedge p}, \mathcal{O}_{C\otimes M^{\wedge p}}) \to M^{\wedge p}$$

induced by Serre duality and to consider a similar map

$$\langle\ ,\omega\rangle : H^1(\mathcal{U}, \mathcal{O}_{C^{\wedge p}}) \to M^{\wedge p}$$

in case we have a prepared covering $\mathcal{U} = (U_i)$ of C (which we also view as a covering of $C \otimes M^{\wedge p}$ and of $C^{\wedge p}$). Let Z and V_P be as in Section 3.6 above. Let us fix an index j_0. Moreover, for any point $P \in Z$ choose an index i_P such that $P \in U_{i_P}$.

For any cocycle $(\eta_{ij}) \in Z^1(\mathcal{U}, \mathcal{O}_{C\otimes M^{\wedge p}})$, $\eta_{ij} \in \mathcal{O}(U_{ij}) \otimes M^{\wedge p}$, representing a class $\eta \in H^1(C \otimes M^{\wedge p}, \mathcal{O}_{C\otimes M^{\wedge p}})$ one defines the Serre pairing

$$\langle \eta, \omega\rangle = \sum_{P\in Z} Res_P(\eta_{i_P j_0}\omega) \in M^{\wedge p}.$$

Of course, changing j_0, as well as changing the choice $P \mapsto i_P$, does not change the value of the above expression.

Similarly assume $(\hat{\eta}_{ij}) \in Z^1(\mathcal{U}, \mathcal{O}_{C^{\wedge p}})$ is a cocycle, $\hat{\eta}_{ij} \in \mathcal{O}(U_{ij})^{\wedge p}$; we define, using Section 3.5,

$$\langle(\hat{\eta}_{ij}), \omega\rangle = \sum_{P\in Z} Res_P(\hat{\eta}_{i_P j_0}\omega) \in M^{\wedge p}.$$

We claim that the two definitions are compatible in the following sense. First there is a canonical homomorphism

$$(*) \qquad Z^1(\mathcal{U}, \mathcal{O}_{C^{\wedge p}}) \to H^1(C \otimes M^{\wedge p}, \mathcal{O}_{C\otimes M^{\wedge p}})$$

which can be described as follows. If $(\hat{\eta}_{ij}) \in Z^1(\mathcal{U}, \mathcal{O}_{C^{\wedge p}})$, then $(\hat{\eta}_{ij})$ induces a compatible system of cocycles in $Z^1(\mathcal{U}, \mathcal{O}_{C\otimes M/(p^\nu)})$, hence a compatible system of classes in $H^1(C \otimes M/(p^\nu), \mathcal{O})$, hence, a class $\eta \in H^1(C \otimes M^{\wedge p}, \mathcal{O})$. Our claim is that

$$\langle \eta, \omega\rangle = \langle(\hat{\eta}_{ij}), \omega\rangle.$$

Indeed, if η is represented by $\eta_{ij} \in Z^1(\mathcal{U}, \mathcal{O}_{C\otimes M^{\wedge p}})$, then for all ν we must have

$$\hat{\eta}_{ij} - \eta_{ij} = f_i^{(\nu)} - f_j^{(\nu)} + p^\nu g_{ij}^{(\nu)}$$

in $\mathcal{O}(U_{ij})^{\wedge p}$, where $f_i^{(\nu)} \in \mathcal{O}(U_i)$ and $g_{ij}^{(\nu)} \in \mathcal{O}(U_{ij})^{\wedge p}$. We conclude that

$$\langle \eta, \omega \rangle - \langle (\hat{\eta}_{ij}), \omega \rangle \in p^\nu M^{\wedge p}$$

for all ν and our claim is checked. By the way, the kernel of the homomorphism $(*)$ above is the group of coboundaries $B^1(\mathcal{U}, \mathcal{O}_{C^{\wedge p}})$; to see this use the surjectivity of the maps

$$H^0(C \otimes M/(p^{\nu+1}), \mathcal{O}) \to H^0(C \otimes M/(p^\nu), \mathcal{O}).$$

The following is an immediate consequence of Section 3.7 and Lemma 3.7:

Corollary 3.9. *Let S be a finite set of primes and let M be a smooth $\mathbf{Z}_S-$algebra. Let C/M be a curve, let $\mathcal{U} = (U_i)$ be a prepared affine open covering of C, and let $\omega \in H^0(C, \Omega_{C/M})$ be a global $1-$form. For each $p \notin S$ let $(\hat{\eta}_{ijp})_{ij} \in Z^1(\mathcal{U}, \mathcal{O}_{C^{\wedge p}})$ be a cocycle and let $\eta_p \in H^1(C \otimes M^{\wedge p}, \mathcal{O}_{C \otimes M^{\wedge p}})$ be its image. Assume that for each i, j the family*

$$(\hat{\eta}_{ijp})_p \in \prod_{p \notin S} \mathcal{O}(U_{ij})^{\wedge p}$$

is formally Fermat. Then the family

$$(\langle \eta_p, \omega \rangle) \in \prod_{p \notin S} M^{\wedge p}$$

is formally Fermat.

Sometimes, upon enlarging S, we may conclude that $(\langle \eta_p, \omega \rangle)$ is Fermat. One such case is given by Proposition 3.4. Another useful instance is given by the following:

Proposition 3.10. *Let S be a finite set of primes and let U and V be affine smooth schemes over $\mathbf{Z}$. Let $V \to U$ be a dominant, generically finite morphism and let t be a finite family of indeterminates. Then there exists a finite set of primes S' containing S and a non-empty Zariski open set $U' \subset U$ with the following property. Let $(f_p) \in \prod_{p \notin S} \mathcal{O}(U)[t]^{\wedge p}$ be such that the image of (f_p) in $\prod_{p \notin S} \mathcal{O}(V)[t]^{\wedge p}$ is formally Fermat; then the image of (f_p) in $\prod_{p \notin S'} \mathcal{O}(U')[t]^{\wedge p}$ in Fermat.*

Proof. Case 1: $V = U$. We may assume $M := \mathcal{O}(U) = (\mathbf{Z}_S[x,y]/(g))_h = \mathbf{Z}_S[x,y,w]/(g, wh-1)$, where $x = \{x_1, ..., x_n\}$, $g \in \mathbf{Z}_S[x,y]$ is monic in y, and $h \in \mathbf{Z}_S[x]$. By enlarging S we may assume, by Proposition 3.4, that any formally Fermat family in $\prod_{p \notin S}(\mathbf{Z}_S[x,t]_h)^{\wedge p}$ is Fermat. Now let

$$(f_p) \in \prod_{p \notin S} M[t]^{\wedge p}$$

be formally Fermat. So if $F_p \in \mathbf{Z}_p[x,y,w,t]^{\wedge p}$ are liftings of f_p, then there exist Fermat families $(F_p^{(\nu)}) \in \prod_{p \notin S} \mathbf{Z}_p[x,y,w,t]^{\wedge p}$ and elements $H_p^{(\nu)}, K_p^{(\nu)}, L_p^{(\nu)} \in \mathbf{Z}_p[x,y,w,t]^{\wedge p}$ such that

$$F_p^{(\nu)} - F_p = H_p^{(\nu)} g + K_p^{(\nu)}(wh-1) + p^\nu L_p^{(\nu)}.$$

Applying the operator $r_g : \mathbf{Z}_p[x,y,w,t]^{\wedge p} \to \mathbf{Z}_p[x,y,w,t]^{\wedge p}$ induced by taking remainders when division by g is performed (where g is viewed as polynomial in y) we obtain

$$(*) \qquad r_g(F_p^{(\nu)}) - r_g(F_p) = r_g(K_p^{(\nu)})(wh-1) + p^\nu r_g(L_p^{(\nu)}).$$

By Remark 2.14, $(r_g(F_p^{(\nu)}))$ is still Fermat. Write

$$r_g(F_p^{(\nu)}) = \sum_{i=0}^{d-1} a_{\nu ip}(x,w,t)y^i, \quad r_g(F_p) = \sum_{i=0}^{d-1} a_{ip}(x,w,t)y^i.$$

By Remark 2.14, again, we get that, for each i, the family $(a_{\nu ip}(x,w,t))$ is Fermat. Picking out coefficients of y^i in $(*)$ and then setting $w \mapsto 1/h$ we get that the family $(a_{ip}(x,1/h,t)) \in \prod_{p\notin S}(\mathbf{Z}[x,t]_h)^{\wedge p}$ is formally Fermat, hence Fermat. We conclude that $f_p = \sum_{i=0}^{d-1} a_{ip}(x,1/h,t)y^i \in \prod_{p\notin S}((\mathbf{Z}[x,y,t]/(g))_h)^{\wedge p}$ is Fermat and we are done.

Case 2: V arbitrary. We may assume $U = Spec\ M$, $V = Spec\ N$, $N := M[z]/(f)$, where $f \in M[z]$ is a monic polynomial of degree d in one variable z. Write $M = \mathbf{Z}[s]/I$, $N = \mathbf{Z}[s,z]/(I,F)$, where s is a tuple of variables, I is some ideal, and F is a monic polynomial in z of degree d mapping to f. Let (f_p) be as in the statement of the proposition. We will show that (f_p) is a formally Fermat family in $\prod_{p\notin S} M[t]^{\wedge p}$; in view of Case 1 in our proof this will close the proof of our proposition. Now we know that (f_p) is a $\mathbf{p}-$adic limit of families $(f_p^{(\nu)})$, $f_p^{(\nu)} \in N[t]^{\wedge p}$ with $f_p^{(\nu)}$ the image of some $F_p^{(\nu)} \in \mathbf{Z}_p[s,z,t]^{\wedge p}$, such that $(F_p^{(\nu)})$ is a Fermat family. By Remark 2.14 we may assume $F_p^{(\nu)} = \sum_{i=0}^{d-1} F_{p,i}^{(\nu)} z^i$, where $F_{p,i}^{(\nu)} \in \mathbf{Z}_p[s,t]^{\wedge p}$. By Remark 2.9 the families $(F_{p,i}^{(\nu)})$ are Fermat, for all i and ν. Let $f_{p,i}^{(\nu)} \in M[t]^{\wedge p}$ be the image of $F_{p,i}^{(\nu)}$. We claim that, for each ν, $(f_{p,0}^{(\nu)})$ converge $\mathbf{p}-$adically to (f_p) and this will close our proof. To check our claim note that $f_p^{(\nu)} = \sum_{i=0}^{d-1} f_{p,i}^{(\nu)} z^i$. Since

$$(f_p^{(\nu)} - f_p) = (f_{p,0}^{(\nu)} - f_p) + (\sum_{i=1}^{d-1} f_{p,i}^{(\nu)} z^i)$$

converges $\mathbf{p}-$adically to (0) and $N[t]^{\wedge p}$ is a free $M[t]^{\wedge p}-$module with basis $1, z, ..., z^{d-1}$, it follows that $(f_{p,0}^{(\nu)} - f_p)$ converges $\mathbf{p}-$adically to (0). □

4. Fermat structure on families of $p-$jet spaces

4.1. Let us quickly review the theory of $p-$jet spaces, as developed in [5], [8]. In what follows p is any prime integer. By a $p-$derivation $\delta : A \to B$ from a ring A into an $A-$algebra B we understand a map satisfying

$$\delta(x+y) = \delta x + \delta y + C_p(x,y),$$
$$\delta(xy) = x^p \delta y + y^p \delta x + p\delta x \delta y,$$

where $C_p(X,Y) := (X^p + Y^p - (X+Y)^p)/p \in \mathbf{Z}[X,Y]$. If δ is a $p-$derivation, then the map $\phi : A \to B$, $\phi(x) := x^p + p\delta x$ is a ring homomorphism. By a *prolongation sequence* we understand a sequence of rings M^n, $n = 1, 2, 3, ...$, such that each M^{n+1} is a M^n-algebra and such that one is given $p-$derivations $\delta_n : M^n \to M^{n+1}$, each δ_n prolonging the previous δ_{n-1}. (By abuse we denote all δ_n by δ.) Prolongation sequences form, in an obvious way, a category. Denote by $\mathbf{Prol}_p$ the full subcategory whose objects are the prolongation sequences M^* for which M^n are Noetherian, $p-$adically complete, and flat over $\mathbf{Z}_p$. An example of an object in $\mathbf{Prol}_p$ that will play a key role later is the following.

Recall that for any prime p we denoted by $\mathbf{Witt}_p$ the class of all complete discrete valuation rings whose maximal ideal is generated by p and whose residue field is perfect; for any $R \in \mathbf{Witt}_p$ we denoted by $\phi : R \to R$ the unique lifting of the $p-$power Frobenius on the residue field and we defined $\delta : R \to R$ by the formula $\delta x := (\phi(x) - x^p)/p$, $x \in R$. The sequence R^* with $R^n := R$ and $p-$derivations as above is a prolongation sequence $R^* \in \mathbf{Prol}_p$.

For any $p-$adically complete ring M^0 let $\mathbf{FSch}_{M^0}$ be the full subcategory of the category of formal schemes over $Spf\ M^0$ whose objects are the formal schemes which are locally $p-$adic completions of schemes of finite type over M^0. Given any $M^* \in \mathbf{Prol}_p$, the theory in [5], [8] provides functors

$$\mathbf{FSch}_{M^0} \to \mathbf{FSch}_{M^r}, \quad X \mapsto J^r(X, M^*),$$

where $J^r(X, M^*)$ is the "$p-$jet space of X of order r" relative to M^*. Let us briefly recall their construction. First, if T is the set of variables $T_1, ..., T_N$, and $T', T'', ..., T^{(r)}, ...$ are new sets of N variables, one defines operators

$$\phi, \delta : M^r[T, T', ..., T^{(r)}]\hat{}^p \to M^{r+1}[T, T', ..., T^{(r+1)}]\hat{}^p$$

by the formulae

$$\phi(f) = f^\phi(T^p + pT', (T')^p + pT'', ..., T^{(r)p} + pT^{(r+1)}),$$
$$\delta f = \frac{\phi(f) - f^p}{p},$$

where f^ϕ is obtained from f by acting with ϕ on the coefficients. (N.B. If $M^0 = \mathbf{Z}_p$, then this δ is entirely different from the δ_p defined in Section 2.2; on the other hand δ can be expressed in terms of $\delta_p, \delta_{T_k}, \delta_{T'_k}, \delta_{T''_k}, ...$ as in Remark 2.18.)

Now if X is affine, equal, say, to $Spf\ M^0[T]\hat{}^p/(f)$ for some tuple f of elements of $M^0[T]\hat{}^p$, then one sets

$$J^r(X, M^*) := Spf\ M^r[T, T', ..., T^{(r)}]\hat{}^p/(f, \delta f, ..., \delta^r f).$$

The latter affine formal scheme depends "functorially" on X and the construction $X \mapsto J^r(X, M^*)$, for affine X, behaves "well" under localization to the effect that this construction extends to a functor $\mathbf{FSch}_{M^0} \to \mathbf{FSch}_{M^r}$. This functor commutes (in the obvious sense) with open immersions and products. If $r = 0$ this functor is the identity.

A special case of this construction is the following. We let $R \in \mathbf{Witt}_p$, let $R^* \in \mathbf{Prol}_p$ be the associated prolongation sequence, let B be a smooth affine scheme over R, and let $M^r := \mathcal{O}(J^r(\hat{B}))$. Then M^* has a natural structure of prolongation sequence in $\mathbf{Prol}_p$ and, for any smooth scheme X/B, we have natural identifications

$$J^r(\hat{X}, M^*) \simeq J^r(\hat{X}, R^*).$$

Also, if $X = X_R$ is an object in $\mathbf{FSch}_R$ we simply write $J^*(X_R)$ instead of $J^*(X_R, R^*)$.

Finally, note that for any morphism $R \to R'$ in $\mathbf{Witt}_p$, any $X_R \in \mathbf{FSch}_R$ and any morphism $P : Spf\ R' \to X_R$ over R, there are natural liftings $P_r : Spf\ R' \to J^r(X_R)$; in affine coordinates, if P is defined by $T_i \mapsto a_i$, then P_r will be defined by $T_i^{(j)} \mapsto \delta^j a_i$.

4.2. For a quick, but systematic, discussion of the functorial aspects of Section 4.1 above we refer to the first section of [8]. (It is shown there that all constructed objects represent appropriate functors.) All we need to know here is that if we have a morphism

$$\tilde{X} = Spf\ M^0[\tilde{T}]^{\hat{}p}/(\tilde{f}) \to X = Spf\ M^0[T]^{\hat{}p}/(f)$$

sending the tuple T mod (f) into a tuple $\tilde{F}$ mod $(\tilde{f})$, where $\tilde{F}$ is a tuple of elements in $M^0[\tilde{T}]^{\hat{}p}$, then the induced map $J^r(\tilde{X}) \to J^r(X)$ sends the tuples

$$T', ..., T^{(r)} \quad mod \quad (f)$$

into the tuples

$$\delta\tilde{F}, ..., \delta^r\tilde{F} \quad mod \quad (\tilde{f}, \delta\tilde{f}, ..., \delta^r\tilde{f}).$$

In particular we have the following specialization principle. Let $R \to R'$ be a morphism in $\mathbf{Witt}_p$ and let $f : X_R \to Y_R$ be a morphisms in $\mathbf{FSch}_R$ and $P : Spf\ R' \to Y_R$ be a point; let $Z_{R'} := X_R \times_{Y_R} Spf\ R'$ be the pull back of X_R via P, let $P_r : Spf\ R' \to J^r(Y_R)$ be the natural lifting of P, and let $f_r : J^r(X_R) \to J^r(Y_R)$ be the map induced by f. Then $J^r(Z_{R'})$ is isomorphic to the pull back of $J^r(X_R)$ via P_r.

From now on, until the end of the paper, we shall assume that S is a finite set of primes containing 2. In Section 6 we shall actually strengthen this condition by insisting that S also contains 3.

4.3. Let X be any scheme of finite type over $\mathbf{Z}_S$, i.e. an object of **Sch**. We can consider the family of its $p-$jet spaces of a given order $(J^r(X^{\hat{}p}))$. We put on this family a Fermat structure, called the *full* Fermat structure, as follows. First we let the index set I be in bijection with the set of all affine open subsets of X (as before, for $i \in I$, we denote by $X_i \subset X$ the corresponding open set and we let $i \leq j$ iff $X_i \subset X_j$). Then, for each p, we set $J^r(X^{\hat{}p})^{(i)} := J^r(X_i{}^{\hat{}p})$ (by compatibility of $p-$jets with open immersions, the latter is simply the pull-back of $X_i{}^{\hat{}p}$ via the projection $J^r(X^{\hat{}p}) \to X^{\hat{}p}$). Finally, for each i, we **choose** an isomorphism $\sigma_i : \mathbf{Z}_S[T]/(f) \simeq \mathcal{O}(X_i)$ (where T is an $N-$ tuple of indeterminates and f is a tuple of polynomials), and we put on $(\mathcal{O}(J^r(X_i{}^{\hat{}p})))$ the Fermat structure defined by the surjections

$$\mathcal{P}(N(r+1))^{\hat{}p} \simeq \mathbf{Z}_p[T, T', ..., T^{(r)}]^{\hat{}p} \to \mathcal{O}(J^r(X_i{}^{\hat{}p}))$$

induced from Section 4.1. We get in this way an object of $\mathcal{F}$**Sch**. If one changes the collection of isomorphisms (σ_i) one obtains a new object of $\mathcal{F}$**Sch**, isomorphic to the original one.

Note that by Remark 2.18 (here we are using the fact that $2 \in S$) and by the Composition axiom, if $(f_p) \in \mathcal{F}(N(r+1))$, then $(\delta f_p) \in \mathcal{F}(N(r+2))$ and so we also have $(\phi f_p) \in \mathcal{F}(N(r+2))$.

If we are given a morphism of $\mathbf{Z}_S-$schemes of finite type $X \to Y$, then one checks immediately, using Section 4.2, that the induced family

$$(J^r(X^{\hat{}p}) \to J^r(Y^{\hat{}p}))$$

is a Fermat family, hence it gives a morphism in $\mathcal{F}$**Sch**. Note also that the natural families of projections $(J^{r+1}(X^{\hat{}p}) \to J^r(X^{\hat{}p}))$ are morphisms in $\mathcal{F}$**Sch**.

Once we fix, for each X in **Sch**, a collection of isomorphisms (σ_i) as above one gets a functor

$$\mathbf{Sch} \to \mathcal{F}\mathbf{Sch}, \quad X \mapsto (J^r(X^{\hat{}p}))_{full}.$$

For $r = 0$ this is the functor in Section 3.2. The index *full* indicates that we are considering the full Fermat structures. On the other hand if X is affine, then the construction above gives a Fermat structure on $\mathcal{O}(J^r(X^{\hat{}p}))$, hence an object $(J^r(X^{\hat{}p}))_{coarse}$ of $\mathcal{F}\mathbf{Sch}_{coarse}$.

We will often consider the following situation. Let $X \to B$ be a morphism in **Sch** with B affine. Then, on the family $(Y_p = X^{\hat{}p} \times_{B^{\hat{}p}} J^r(B^{\hat{}p}))$ we may consider the following Fermat structure (called *induced from* X and denoted by $(Y_p)_{ind,X}$). The index set I is in bijection with the set of all open affine subsets X_i of X, and for all $i \in I$ we let $Y_p^{(i)} = X_i{}^{\hat{}p} \times_{B^{\hat{}p}} J^r(B^{\hat{}p})$ have its ring of functions be equipped with the product Fermat structure. (Of course, if $B = Spec\ \mathbf{Z}_S$, then $Y_p = X^{\hat{}p}$.) More generally, in a similar way, if Z is an affine scheme in **Sch** one can consider the Fermat structure $(Y_p \times Z^{\hat{}p})_{ind,X}$ *induced* from X.

Recall from [5] that for any r and any formal scheme X_R, smooth over $R \in \mathbf{Witt}_p$, the projection $J^r(X_R) \to X_R$ is locally, in the Zariski topology, a trivial bundle with fiber $(\mathbf{A}^{nr})^{\hat{}p}$, the completion of the affine space of dimension nr, where n is the relative dimension of X_R/R. (Here a formal scheme over R is called *smooth* if it is locally obtained by $p-$adically completing a smooth scheme over R. More generally a morphism of formal schemes will be called smooth if it is the $p-$adic completion of a smooth morphism of schemes of finite type over R.) Moreover these bundles for various r's are compatible with each other in the obvious sense.

The following more precise statement follows from [5], p. 317, and will be needed. Assume $M^* \in \mathbf{Prol}_p$ and let U be a smooth scheme over M^0. By *etale coordinates* on U/M^0 we understand here an $m-$tuple of elements of $\mathcal{O}(U)$ such that the induced map $U \to \mathbf{A}^m_{M^0}$ is etale. Then the following holds: if U/M^0 admits etale coordinates y, then $J^r(\hat{U}, M^*)$ is naturally isomorphic to $\hat{U} \times_{Spf\ M^0} Spf\ M^r \times \hat{\mathbf{A}}^{mr}$ such that the coordinates on $\mathbf{A}^{mr}$ are given by $\delta y, ..., \delta^r y$.

In what follows we want to show that the above "local trivialisations" can be made "Fermat".

Let $U \to B$ be a smooth morphism of smooth affine schemes over $\mathbf{Z}_S$. We say that U/B has *special etale coordinates* if

$$\mathcal{O}(B) = \mathbf{Z}_S[T_1, ..., T_m]/(g),$$
$$\mathcal{O}(U) = (\mathbf{Z}_S[T_1, ..., T_{n+1}]/(g, f))_{(\partial f/\partial T_{n+1})G},$$

where g is a tuple of polynomials in $\mathbf{Z}_S[T_1, ..., T_m]$, and f, G are polynomials in $\mathbf{Z}_S[T_1, ..., T_{n+1}]$. The images of $T_{m+1}, ..., T_n$ in the ring above will be called the *special etale coordinates* in this representation. (Our special etale coordinates are, of course, directly related to the *special affine varieties* of Monski-Washnitzer [21].)

If B is integral and X/B is any smooth scheme over B, then, after replacing B by a non-empty affine open set of it, X can be covered with affine open sets X_i such that, for each i, X_i/B has special etale coordinates. (This follows, for instance, by combining the various results in [4], Chapter 2.)

We will prove the following:

Proposition 4.1. *Let U/B have special etale coordinates as above. Let $Y_p = U^{\hat{}p} \times_{B^{\hat{}p}} J^r(B^{\hat{}p})$. Then we have the following isomorphisms in $\mathcal{F}\mathbf{Sch}$:*

1) $(J^r(U^{\hat{}p}))_{full} \simeq (Y_p \times (\mathbf{A}^{r(n-m)})^{\hat{}p})_{ind,U}$ *over* $(Y_p)_{ind,U}$.

2) $(J^r(U^{\hat{}p}))_{coarse} \simeq (Y_p \times (\mathbf{A}^{r(n-m)})^{\hat{}p})_{coarse}$ *over* $(Y_p)_{coarse}$.

To prove the proposition we need some preparation.

Lemma 4.2. *Let $x_0, ..., x_d, u, w, v$ be indeterminates and consider the polynomial*

$$\Phi(x, u, v) = x_0 + x_1 u + v x_2 u^2 + ... + v x_d u^d \in \mathbf{Z}[x, u, v],$$

where x is the $d+1-$tuple $x_0, ..., x_d$. Then there exists a power series $\Psi_d := \Psi(x, w, v) \in \mathbf{Z}[x, w][[v]]$ such that

$$\Phi(x, \Psi(x, x_1^{-1}, v), v) = 0$$

in the ring $\mathbf{Z}[x, x_1^{-1}][[v]]$.

Proof. Standard, in the style of Hensel's Lemma. □

Lemma 4.3. *For any $f \in \mathbf{Z}_p[T]$, where T is a tuple of variables (T_i), the following formula holds in the ring $\mathbf{Z}_p[T, T', ..., T^{(r)}]$:*

$$\frac{\partial(\delta^r f)}{\partial T_i^{(r)}} = \phi^r \left(\frac{\partial f}{\partial T_i} \right).$$

Proof. An easy exercise; or use Lemma 2.3 in [6], p.361, plus induction. □

Proof of Proposition 4.1. Write

$$\mathcal{O}(U) = \mathbf{Z}_S[T_1, ..., T_{n+1}, T_{n+2}]/(g, f, 1 - T_{n+2} G(\partial f / \partial T_{n+1}))$$

(cf. the paragraph before the statement of Proposition 4.1). Let t denote the tuple $T_1, ..., T_n$. Then, for $i \geq 1$, one can check by induction that one can write

$$\delta^i f = \sum_{j=0}^{d} a_{ijp} T_{n+1}^{(i)j}, \quad a_{ijp} \in \mathbf{Z}_p[t, t', ..., t^{(i)}, T_{n+1}, T'_{n+1}, ..., T_{n+1}^{(i-1)}]^{\wedge p},$$

where d is the degree of f in T_{n+1}. Since, for each i, $(\delta^i f)$ is a Fermat family, it follows that for each i, (a_{i0p}) is a Fermat family. By Lemma 4.3 we have

$$a_{i1p} = \phi^i \left(\frac{\partial f}{\partial T_{n+1}} \right)_{|T_{n+1}^{(i)} = 0}.$$

On the other hand we claim that we have

$$\phi^i \left(\frac{\partial f}{\partial T_{n+1}} \right) = \left(\frac{\partial f}{\partial T_{n+1}} \right)^{p^i} + p D_{ip},$$

where (D_{ip}) is a Fermat family. Indeed, it follows from Remark 2.15 that we can write an equation as above where D_{ip} is obtained from a Fermat family in $\mathcal{F}$ by substituting the variables by

$$\frac{\partial f}{\partial T_{n+1}}, \delta \left(\frac{\partial f}{\partial T_{n+1}} \right), ..., \delta^i \left(\frac{\partial f}{\partial T_{n+1}} \right);$$

this proves our claim. Setting $T_{n+1}^{(i)} = 0$ in the last equation and using the Composition axiom we get that

$$a_{i1p} = \left(\frac{\partial f}{\partial T_{n+1}} \right)^{p^i} + p d_{ip}$$

with (d_{ip}) a Fermat family. On the other hand one sees by induction on i that for all $i \geq 1$ and all $j \geq 2$ we have that $a_{ijp} = p b_{ijp}$ with (b_{ijp}) a Fermat family.

The same arguments as above applied to $1-T_{n+2}(df/dT_{n+1})G$ in place of f and T_{n+2} in place of T_{n+1} show that

$$\delta^i(1-T_{n+2}(\partial f/\partial T_{n+1})G)=\alpha_{ip}+[(\partial f/\partial T_{n+1})^{p^i}G^{p^i}+p\beta_{ip}]T_{n+2}^{(i)},$$

where α_{ip},β_{ip} do not depend on $T_{n+2}^{(i)}$ and form Fermat families.

Let T denote the tuple $T_1,...,T_{n+1}$ and $\tilde{T}$ denote the tuple $T_1,...,T_{n+2}$. We shall define a Fermat family of isomorphisms between the family of rings

$$(*)_G \qquad \mathbf{Z}_p[\tilde{T},...,\tilde{T}^{(r)}]^{\wedge p}/(\delta^i g,\delta^i f,\delta^i(1-T_{n+2}(\partial f/\partial T_{n+1})G)$$

and the family of rings

$$(**)_G \qquad \mathbf{Z}_p[\tilde{T},t',...,t^{(r)}]^{\wedge p}/(\delta^i g,f,1-T_{n+2}(\partial f/\partial T_{n+1})G),$$

where i above runs through $0,...,r$. This will, of course, close the proof of statement 2) in the proposition.

There is an obvious Fermat family of morphisms $(**)_G\to(*)_G$ given by $\tilde{T}\mapsto\tilde{T}$, $t^{(i)}\mapsto t^{(i)}$ and it is easy to see that these are ring isomorphisms. What is not clear a priori is that the inverse morphisms $(*)_G\to(**)_G$ form a Fermat family. We shall explicitly provide a Fermat inverse. Let Ψ be the series in Lemma 4.2. Then we define morphisms from $(*)_G\to(**)_G$ by sending $\tilde{T}\mapsto\tilde{T}$, $T_{n+2}\mapsto T_{n+2}$ and, for $i\geq 1$:

$$T_{n+2}^{(i)}\mapsto -\alpha_{ip}\sum_{j=0}^{\infty}(-1)^j p^j\beta_{ip}^j T_{n+2}^{p^i(j+1)},$$

$$T_{n+1}^{(i)}\mapsto\Psi(a_{i0p},a_{i1p},b_{i2p},...,b_{idp},\eta_{ip},p),$$

where

$$\eta_{ip}:=\sum_{j=0}^{\infty}(-1)^j p^j d_{ip}^j G^{p^i(j+1)}T_{n+2}^{p^i(j+1)}.$$

(Of course these formulae are obtained by "solving the equations $\delta^i f=0$ and $\delta^i(1-T_{n+2}(\partial f/\partial T_{n+1})G)=0$" for the variables $T_{n+1}^{(i)}$ and $T_{n+2}^{(i)}$, respectively.) Obviously the homomorphisms we defined form Fermat families, and our proof of assertion 2) in Proposition 4.1 is concluded.

To check assertion 1) in Proposition 4.1 we need to prove that the induced family of morphisms $(J^r(U^{\wedge p})\to(Y_p\times(\mathbf{A}^{r(n-m)})^{\wedge p})$ as well as their inverses are Fermat families, when one considers the full Fermat structures. It is enough to check that for any $H\in\mathbf{Z}_S[\tilde{T}]$ we have an isomorphism between the corresponding rings $(*)_{GH}$ and $(**)_{GH}$ compatible with $(*)_G\simeq(**)_G$. Since G in our discussion was completely arbitrary we could replace G by GH everywhere and get the desired isomorphism. Compatibility with $(*)_G\simeq(**)_G$ is also clear. This closes the proof of Proposition 4.1.

4.4. As the proof of Proposition 4.1 shows, if $\tau=(T_{m+1},...,T_n)$ give special etale coordinates on U in some representation, then the isomorphism $(*)_G$ in Proposition 4.1 can be arranged to send $\tau',...,\tau^{(r)}$ into the coordinate functions on $(\mathbf{A}^{r(n-m)})^{\wedge p}$. There is, of course, only one family of isomorphisms as in Proposition 4.1 satisfying this additional property; we call this unique family the *canonical trivialisation* of $(J^r(U^{\wedge p}))$ attached to the special etale coordinates on U. On the other hand the isomorphisms in Proposition 4.1 constructed for various r's will be compatible with each other in the obvious sense.

The statement of Proposition 4.1 immediately suggests the following general questions. First: does an isomorphism in $\mathcal{F}\mathbf{Sch}$ between objects with full Fermat structures imply (under certain conditions) an isomorphism for coarse Fermat structures? Second: is the converse (sometimes) true? Proposition 3.2 should be viewed as dealing, in a quite special case, with the first question, for Proposition 3.2 is really about Fermat families of morphisms to $((\mathbf{A}^1)^{\wedge p})$. As to the second question one can also prove results in special cases which will play a role later; this will be explained in what follows.

Let $U = Spec\ A$ be an affine scheme of finite type over $\mathbf{Z}_S$ and assume we are given a morphism $(\pi_p) : (X_p) \to (U^{\wedge p})$ in $\mathcal{F}\mathbf{Sch}$ where all X_p are affine and $(U^{\wedge p})$ is viewed with its full Fermat structure. We say that (X_p) is *affine* over $(U^{\wedge p})$ if the index set for (X_p) coincides as an ordered set with the index set I for $(U^{\wedge p})$ (i.e. with the set of affine open sets of U), and for any affine open set $U_i \subset U$ we have $X_p^{(i)} = \pi_p^{-1}(U_i{}^{\wedge p})$. Note that if this is the case, then $(\mathcal{O}(X_p))$ comes with a Fermat structure, so we can also equip (X_p) with a coarse Fermat structure to get an object $(X_p)_{coarse}$ in $\mathcal{F}\mathbf{Sch}_{coarse}$.

Now assume (X_p) is affine over $(U^{\wedge p})$. Then for any principal open set $U_i = Spec\ A_f$ of U we have a natural isomorphism

$$(*) \qquad \mathcal{O}(X_p^{(i)}) = \mathcal{O}(\pi_p^{-1}(U_i{}^{\wedge p})) \to (\mathcal{O}(X_p)_f)^{\wedge p}.$$

Now $(\mathcal{O}(X_p^{(i)}))$ comes with a Fermat structure (by the definition of a Fermat structure on (X_p)). On the other hand $((\mathcal{O}(X_p)_f)^{\wedge p})$ has a Fermat structure naturally induced from the Fermat structure

$$(**) \qquad \mathcal{P}(n)^{\wedge p} \to \mathcal{O}(X_p)$$

by considering the lifting of $(**)$ to surjections

$$(***) \qquad \mathcal{P}(n+1)^{\wedge p} \to (\mathcal{O}(X_p)_f)^{\wedge p}, \quad x_{n+1} \mapsto 1/f.$$

We will say that (X_p) is *principal* over $(U^{\wedge p})$ if (it is affine over $(U^{\wedge p})$ and) the family of isomorphisms $(*)$ as well as the family of their inverses are Fermat (with respect to the two Fermat structures described above).

Note that if $X \to U$ is an affine morphism in $\mathbf{Sch}$, then $(X^{\wedge p})_{ind}$ (where *ind* means "Fermat structure induced from U") is principal over $(U^{\wedge p})$.

Proposition 4.4. *Assume $U \to V$ is a morphism in* $\mathbf{Sch}$. *Assume (X_p) and (Y_p) are principal over $(U^{\wedge p})$ and $(V^{\wedge p})$, respectively, and assume we have a morphism*

$$(X_p)_{coarse} \to (Y_p)_{coarse}$$

in $\mathcal{F}\mathbf{Sch}_{coarse}$, compatible with $U \to V$. Then we have induced morphisms

$$(X_p^{(i)})_{coarse} \to (Y_p^{(j)})_{coarse}$$

in $\mathcal{F}\mathbf{Sch}_{coarse}$ for all principal open subsets $U_i \subset U$, $V_j \subset V$ such that U_i is mapped into V_j. Consequently we have an induced morphism in $\mathcal{F}\mathbf{Sch}$

$$(X_p) \to (Y_p).$$

Proof. A trivial exercise. □

Proposition 4.5. 1) *Let U be an affine scheme of finite type over $\mathbf{Z}_S$. Then $(J^r(U^{\wedge p}))$ is principal over $(U^{\wedge p})$.*

2) *Let $U \to B$ be a morphism of affine schemes in* **Sch**. *Then*

$$(U^{\wedge p} \times_{B^{\wedge p}} J^r(B^{\wedge p}))_{ind,U}$$

is principal over $(U^{\wedge p})$.

Proof. Assertion 2) is trivial. To prove assertion 1 write $U = Spec\ \mathbf{Z}_S[T]/(f)$, where $T = \{T_1, ..., T_N\}$ is an $N-$tuple of variables and f is a tuple of polynomials. Let U_i be the principal open set of U defined by some $G \in \mathbf{Z}_S[T]$, hence

$$\mathcal{O}(U_i) = \mathbf{Z}_S[T, T_{N+1}]/(f, T_{N+1}G - 1).$$

We must prove that there is a Fermat family of isomorphisms (σ_p) from

$$\mathbf{Z}_p[T, ..., T^{(r)}, T_{N+1}, ..., T_{N+1}^{(r)}]^{\wedge p}/(\delta^i f, \delta^i(T_{N+1}G - 1); 0 \leq i \leq r)$$

to

$$\mathbf{Z}_p[T, ..., T^{(r)}, T_{N+1}]^{\wedge p}/(\delta^i f, T_{N+1}G - 1; 0 \leq i \leq r)$$

with respect to the Fermat structures obtained by mapping the numerators of the rings above into those rings such that the family (σ_p^{-1}) is also Fermat. This can be done by looking back at the proof of Proposition 4.1 were the necessary Fermat families of series were actually already constructed. □

By the last two propositions we get:

Corollary 4.6. *Let $U \to B$ be a morphism of affine schemes in* **Sch** *and assume one has a section*

$$(U^{\wedge p} \times_{B^{\wedge p}} J^r(B^{\wedge p}))_{coarse} \to (J^r(U^{\wedge p}))_{coarse}$$

in $\mathcal{F}\mathbf{Sch}_{coarse}$ of the natural projection. Then there is an induced morphism

$$(U^{\wedge p} \times_{B^{\wedge p}} J^r(B^{\wedge p}))_{ind,U} \to (J^r(U^{\wedge p}))_{full}$$

in $\mathcal{F}\mathbf{Sch}$ and also morphisms

$$(U_i{}^{\wedge p} \times_{B^{\wedge p}} J^r(B^{\wedge p}))_{coarse} \to (J^r(U_i{}^{\wedge p}))_{coarse}$$

in $\mathcal{F}\mathbf{Sch}_{coarse}$ for all affine principal open sets $U_i \subset U$.

4.5. Here is a consequence of Corollary 4.6. Let $U \to B$ be as in Corollary 4.6 and let

$$(\alpha_p), (\beta_p) : (U^{\wedge p} \times_{B^{\wedge p}} J^r(B^{\wedge p}))_{coarse} \to (J^r(U^{\wedge p}))_{coarse}$$

be sections in $\mathcal{F}\mathbf{Sch}$ "over B". Then, by the discussion in Section 3.1 about tensor products, there is an induced morphism

$$(\alpha_p \times \beta_p) : (U^{\wedge p} \times_{B^{\wedge p}} U^{\wedge p} \times_{B^{\wedge p}} J^r(B^{\wedge p}))_{coarse} \to (J^r(U^{\wedge p}) \times_{J^r(B^{\wedge p})} J^r(U^{\wedge p}))_{coarse}.$$

Since $J^r(U^{\wedge p}) \times_{J^r(B^{\wedge p})} J^r(U^{\wedge p}) = J^r((U \times_B U)^{\wedge p})$, it follows from Corollary 4.6 that we get an induced morphism

$$((U \times_B U)^{\wedge p} \times_{B^{\wedge p}} J^r(B^{\wedge p}))_{ind,U \times_B U} \to (J^r((U \times_B U)^{\wedge p}))_{full}.$$

We will need the following variant of Proposition 4.1:

Proposition 4.7. *Let M be a finitely generated $\mathbf{Z}_S-$algebra and*

$$B = Spec\ M, \quad U = Spec\ M[x, y]/(f),$$

where f is a polynomial in two variables, of degree d, such that

$$\left(f, \frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}\right) = (1).$$

Then, for any r, there is a section in $\mathcal{F}\mathbf{Sch}$

$$(U^{\wedge p} \times_{B^{\wedge p}} J^r(B^{\wedge p}))_{coarse} \to (J^r(U^{\wedge p}))_{coarse}$$

of the natural projection.

Note that, unlike in Proposition 4.1, we do not assume there are special etale coordinates on U. The existence, for each p, of a section was noted by Hurlburt [15]; what Proposition 4.7 says is that one can choose these sections to form "Fermat families". We need the following:

Lemma 4.8. *Let $x_0, x_1, x_2, x_{ij}, u_1, u_2, s_1, s_2, w, v$ be indeterminates (where $2 \leq i+j \leq d$, $i, j \geq 0$) and consider the polynomial*

$$\Phi(x, u, v) = x_0 + x_1u_1 + x_2u_2 + v \cdot \sum_{i+j=0}^{d} x_{ij}u_1^i u_2^j \in \mathbf{Z}[x, u, v]$$

(where x is the tuple (x_0, x_1, x_2, x_{ij}) and $u = (u_1, u_2)$). Then there exists a pair $\Psi = (\Psi_{1d}, \Psi_{2d})$ of series

$$\Psi_{id} = \Psi_{id}(x, s_1, s_2, w, v) \in \mathbf{Z}[x, s_1, s_2, w][[v]], \quad i = 1, 2,$$

such that

$$\Phi(x, \Psi(x, s_1, s_2, (s_1x_1 + s_2x_2)^{-1}, v), v) = 0$$

in the ring $\mathbf{Z}[x, s_1, s_2, (s_1x_1 + s_2x_2)^{-1}][[v]]$.

Proof. Standard, in the style of Hensel's lemma. □

Proof of Proposition 4.7. Let $M = \mathbf{Z}_S[t]/(g)$, where t is a tuple of variables and g is a tuple of polynomials. If d is the degree of f, then, as in the proof of Proposition 4.1, one can write, for all $k \leq r$,

$$\delta^k f = a_{0kp} + a_{1kp}x^{(k)} + a_{2kp}y^{(k)} + p \sum_{i+j=2}^{d} \alpha_{ijkp}(x^{(k)})^i (y^{(k)})^j$$

with $a_{0kp}, a_{1kp}, a_{2kp}, \alpha_{ijkp} \in \mathbf{Z}_p[t, x, y, ..., t^{(k-1)}, x^{(k-1)}, y^{(k-1)}, t^{(k)}]^{\wedge p}$ forming, as p varies, Fermat families. As in Proposition 4.1 one finds that

$$a_{1kp} = \left(\frac{\partial f}{\partial x}\right)^{p^k} + pd_{1kp},$$

$$a_{2kp} = \left(\frac{\partial f}{\partial y}\right)^{p^k} + pd_{2kp},$$

where (d_{1kp}) and (d_{2kp}) are Fermat families. Write

$$h_1\frac{\partial f}{\partial x} + h_2\frac{\partial f}{\partial y} + hf = 1$$

with $h_1, h_2, h \in \mathbf{Z}_S[t, x, y]$. By Remark 2.17 there exist Fermat families (A_{1kp}) and (A_{2kp}) of polynomials in x_1, x_2 with $\mathbf{Z}-$coefficients such that

$$(x_1 + x_2)^{2p^k} = A_{1kp}x_1^{p^k} + A_{2kp}x_2^{p^k}.$$

We then have

$$(1 - hf)^{2p^k} = H_{1kp}\left(\frac{\partial f}{\partial x}\right)^{p^k} + H_{2kp}\left(\frac{\partial f}{\partial y}\right)^{p^k},$$

where

$$H_{ikp} = A_{ikp}(h_1\frac{\partial f}{\partial x}, h_2\frac{\partial f}{\partial y})h_i^{p^k}, \quad i = 1, 2,$$

are obviously Fermat families. Denote by a_{kp} the tuple

$$(a_{0kp}, a_{1kp}, a_{2kp}, \alpha_{ijkp}).$$

Let Ψ_i be the series defined in Lemma 4.8. Then we may consider the Fermat family of ring homomorphisms

$$\mathbf{Z}_p[t, x, y, ..., t^{(r)}, x^{(r)}, y^{(r)}]\hat{}^p/(g, \delta g, ..., \delta^r g, f, \delta f, ..., \delta^r f)$$
$$\to \mathbf{Z}_p[t, x, y, t', ..., t^{(r)}]\hat{}^p/(g, \delta g, ..., \delta^r g, f)$$

defined by $t^{(i)} \mapsto t^{(i)}$, $x \mapsto x$, $y \mapsto y$ and

$$x^{(k)} \mapsto \Psi_{1d}(a_{kp}, H_{1kp}, H_{2kp}, \theta_{kp}, p),$$
$$y^{(k)} \mapsto \Psi_{2d}(a_{kp}, H_{1kp}, H_{2kp}, \theta_{kp}, p),$$

where

$$\theta_{kp} := \sum_{n=0}^{\infty}(-1)^n p^n (H_{1kp}d_{1kp} + H_{2kp}d_{2kp})^n,$$

and we are done.

5. Fermat families arising from formal groups

5.1. Let $B = Spec\ M$, where M is either a smooth $\mathbf{Z}_S-$algebra, where S is a finite set of primes, or M is any Noetherian, flat $\mathbf{Z}_p-$algebra. In the first situation we say we are in the global case whereas in the second situation we say we are in the local case. We will later need to consider both cases. Let z be a $g-$tuple of variables and consider $g-$tuples of variables $z', z'', ..., z^{(r)}, ...$ In the global case set $M_p^r = \mathcal{O}(J^r(B\hat{}^p))$ (where p varies outside S); so, for each p, $M_p^* \in \mathbf{Prol}_p$. In the local case assume we are given a prolongation sequence $M_p^* \in \mathbf{Prol}_p$ such that $M_p^0 = \hat{M}$. There are unique ring homomorphisms

$$M_p^0[[z]] \xrightarrow{\phi} M_p^1[[z, z']] \xrightarrow{\phi} M_p^2[[z, z', z'']] \xrightarrow{\phi} ...$$

such that $\phi(t) = t^p + p\delta t$ for $t \in M_p^r$ and such that $\phi(z^{(r)}) = (z^{(r)})^p + pz^{(r+1)}$. As a notational rule, if $f \in M_p^r[[z, z', ..., z^{(r)}]]$, then f^{ϕ^i} will mean the series obtained from f by "acting its coefficients with ϕ^i". Now define maps

$$M_p^0[[z]] \xrightarrow{\delta} M_p^1[[z, z']] \xrightarrow{\delta} M_p^2[[z, z', z'']] \xrightarrow{\delta} ...$$

by the formula $\delta(f) := (\phi(f) - f^p)/p$. Note that ϕ and δ commute.

Here is one more useful notation: if $F, g_0, ..., g_r \in (M_p^r[[z, z', ..., z^{(r)}]])^g$ are $g-$tuples of series and either $F \in (M_p^r[z, ..., z^{(r)}]\hat{}^p)^g$ or all $g_i \in (z, ..., z^{(r)})^g$, then we denote by $[F]\circ[g_0, ..., g_r] \in (M_p^r[[z, z', ..., z^{(r)}]])^g$ the result obtained by replacing $z, z', ..., z^{(r)}$ in F by $g_0, ..., g_r$; in other words $[F] \circ [g_0, ..., g_r] := F(g_0, ..., g_r)$. With this convention it is trivial to check, by induction, that for any $G \in M[[z]]^g$ we have

$$(*) \qquad [\phi^r(z)] \circ [G, \delta G, ..., \delta^r G] = \phi^r(G).$$

Also, by induction, one sees that the components of the vector $\phi^r(z) - z^{p^r} - p(z')^{p^{r-1}}$ belong to the ideal (pz, p^2); consequently we have

$$(**) \qquad [\phi^r(z)] \circ [0, z', ..., z^{(r)}] \equiv 0 \mod (p),$$
$$\frac{1}{p}[\phi^r(z)] \circ [0, z', ..., z^{(r)}] \equiv (z')^{p^{r-1}} \mod (p).$$

Next we claim that if $F \in M[[z]]^g$, $F(0) = 0$, then

$$(***) \qquad [\delta^r F] \circ [0, z', ..., z^{(r)}] \in (M_p^r[z', ..., z^{(r)}]^{\wedge p})^g$$

i.e. the components of the above vector are restricted power series (rather than merely formal power series). Indeed (as one can check by induction) the $i-$th component of $p^r \delta^r F$ belongs to the ring generated by the $i-$th components of $F, \phi(F), ..., \phi^r(F)$ so it is enough to check that the components of

$$[\phi^r(F)] \circ [0, z', ..., z^{(r)}]$$

are restricted power series. But

$$[\phi^r(F)] \circ [0, z', ..., z^{(r)}] = [F^{\phi^r}] \circ [\phi^r(z)] \circ [0, z', ..., z^{(r)}]$$

and we are done by $(**)$ above.

We will also need the following formula, valid for any invertible element $\lambda \in M^\times$:

$$(****) \qquad [\phi^r(z)] \circ [0, z', ..., z^{(r)}] \circ [\delta(\lambda^{-1}z), ..., \delta^r(\lambda^{-1}z)] \circ [0, z', ..., z^{(r)}]$$
$$= [\phi^r(\lambda^{-1})\phi^r(z)] \circ [0, z', ..., z^{(r)}].$$

Indeed, the left-hand side of the above equation equals

$$[\phi^r(z)] \circ [0, \delta(\lambda^{-1}z), ..., \delta^r(\lambda^{-1}z)] \circ [0, z', ..., z^{(r)}]$$
$$= [\phi^r(z)] \circ [\lambda^{-1}z, \delta(\lambda^{-1}z), ..., \delta^r(\lambda^{-1}z)] \circ [0, z', ..., z^{(r)}].$$

By $(*)$ above the latter equals

$$[\phi^r(\lambda^{-1}z)] \circ [0, z', ..., z^{(r)}] = \phi^r(\lambda^{-1})[\phi^r(z)] \circ [0, z', ..., z^{(r)}].$$

5.2. Let $\Phi(z_1, z_2) \in (M[[z_1, z_2]])^g$ be a commutative formal group in g variables (so here z_1, z_2 are $g-$tuples of variables) and consider the associated logarithm

$$l(z) = \sum_{|\mathbf{n}| \geq 1} a_{\mathbf{n}} z^{\mathbf{n}},$$

where $\mathbf{n}$ are $g-$tuples of non-negative integers with sum $|\mathbf{n}|$, and $a_{\mathbf{n}} \in (M \otimes \mathbf{Q})^g$ are viewed as column vectors. We then have

$$\Phi(z_1, z_2) = e(l(z_1) + l(z_2)),$$

where $e(z) \in ((\mathbf{Q} \otimes M)[[z]])^g$ is the exponential, i.e. the compositional inverse of $l(z)$. Then the $(r+1)g-$tuple of formal series $(\Phi, \delta\Phi, ..., \delta^r\Phi)$ in the variables $\mathbf{z} = (z_1, z_2)$, $\mathbf{z}' = (z_1', z_2')$,..., $\mathbf{z}^{(r)} = (z_1^{(r)}, z_2^{(r)})$ is a (commutative) formal group law in $(r+1)g$ variables. Let us set $\mathbf{z} = 0$ in this tuple, in other words consider the $rg-$tuple

$$([\delta\Phi] \circ [0, \mathbf{z}', ..., \mathbf{z}^{(r)}], ..., [\delta^r\Phi] \circ [0, \mathbf{z}', ..., \mathbf{z}^{(r)}]).$$

By $(***)$ in Section 5.1 the components of the latter tuple are restricted power series (rather than mere formal power series) i.e. belong to $M_p^r[\mathbf{z}', ..., \mathbf{z}^{(r)}]^{\wedge p}$. In particular this $rg-$tuple makes the completed affine space $(\mathbf{A}^{rg})^{\wedge p}$ into a group

object in the category $\mathbf{FSch}_{M_p^r}$. Denote by $[+]$ the addition on this completed affine space.

Now define, for each p, and each $r \geq 1$, the following $g-$tuple of series

$$L_p^r = L_p^r(z', ..., z^{(r)}) := \frac{1}{p}[l^{\phi^r}] \circ [\phi^r(z)] \circ [0, z', ..., z^{(r)}].$$

(Division by p in unambiguous because M_p^r is flat over $\mathbf{Z}_p$.) By $(**)$ in Section 5.1 the components of this tuple belong to $M_p^r[z', ..., z^{(r)}]^{\wedge p}$.

Proposition 5.1. *In the global case (L_p^r) are Fermat. Also, in both the global and the local case, $L_p^r \equiv (z')^{p^{r-1}}$ mod (p), in particular $L_p^r \equiv (L_p^1)^{p^{r-1}}$ mod (p).*

Here a family of vectors is called Fermat if, for each index i, the family of the $i-$th components is Fermat.

Proof. Since

$$\frac{1}{p}[\phi^r(z)] \circ [0, z', ..., z^{(r)}] = \left[\frac{\phi^r(z) - z^{p^r}}{p}\right] \circ [0, z', ..., z^{(r)}]$$

and since, by Remark 2.18 plus the Composition axiom, the right-hand side of the above equality is, in the global case, Fermat, it follows that so is the left-hand side. Call this left-hand side G_p^r. Then we have

$$L_p^r = \sum_{|\mathbf{n}| \geq 1} \phi^r(a_{\mathbf{n}}) p^{|\mathbf{n}|-1} (G_p^r)^{\mathbf{n}}.$$

By [14], p. 64, (11.1.3) and (11.1.4), we can write

$$a_{\mathbf{n}} = \sum_{t \geq 1} \sum_{p_1 ... p_t || \mathbf{n}|} \frac{A_{p_1, ..., p_t}}{p_1 ... p_t},$$

where $A_{p_1, ..., p_t} \in M^g$ and $p_1, ..., p_t$ run through the set of all (not necessarily distinct) primes such that the product $p_1 ... p_t$ divides $|\mathbf{n}|$. Let v_p be the valuation at $p \neq 2$ on the rationals. We have

$$\mu_p(\mathbf{n}, p_1, ..., p_r) := v_p\left(\frac{p^{|\mathbf{n}|-1}}{p_1 ... p_t}\right) \geq |\mathbf{n}| - 1 - t',$$

where $t' = t - 1$ if at least one of the p_i's equals 2 and $t' = t$ if no p_i equals 2. In the first case $t \leq \frac{log\ |\mathbf{n}|}{log\ 2}$ and in the second case $t \leq \frac{log\ |\mathbf{n}|}{log\ 3}$. So in both cases $|\mathbf{n}| - 1 - t'$ is ≥ 0, and it is ≥ 1 for $|\mathbf{n}| \geq 2$. Moreover, in both cases $|\mathbf{n}| - 1 - t' \geq |\mathbf{n}| - 1 - \frac{log\ |\mathbf{n}|}{log\ 2} \to \infty$ as $|\mathbf{n}| \to \infty$ so, by Remark 2.11 and the $\mathbf{p}-$adic closure axiom, (L_p^r) is Fermat. Also note that, since $l^{\phi^r}(z) \equiv z$ mod $(z)^2$, we get that $L_p^r \equiv (z')^{p^{r-1}}$ mod (p). □

Proposition 5.2. *In both the global and the local case, the $g-$tuple L_p^r defines a group homomorphism*

$$((\mathbf{A}^{rg})^{\wedge p}, [+]) \to (((\mathbf{A})^{\wedge p})^g, +);$$

in other words, the following formula holds:

$$L_p^r((z_1', ..., z_1^{(r)})[+](z_2', ..., z_2^{(r)})) = L_p^r(z_1', ..., z_1^{(r)}) + L_p^r(z_2', ..., z_2^{(r)}).$$

Proof.

$$\begin{aligned}
&L_p^r((z_1', ..., z_1^{(r)}) \oplus (z_2', ..., z_2^{(r)})) \\
&= L_p^r([\delta\Phi] \circ [0, \mathbf{z}', ..., \mathbf{z}^{(r)}], ..., [\delta^r\Phi] \circ [0, \mathbf{z}', ..., \mathbf{z}^{(r)}]) \\
&= \frac{1}{p}[l^{\phi^r}] \circ [\phi^r(z)] \circ [0, [\delta\Phi] \circ [0, \mathbf{z}', ..., \mathbf{z}^{(r)}], ..., [\delta^r\Phi] \circ [0, \mathbf{z}', ..., \mathbf{z}^{(r)}]] \\
&= \frac{1}{p}[l^{\phi^r}] \circ [\phi^r(z)] \circ [\Phi, \delta\Phi, ..., \delta^r\Phi] \circ [0, \mathbf{z}', ..., \mathbf{z}^{(r)}] \\
&= \frac{1}{p}[l^{\phi^r}] \circ [\phi^r(\Phi)] \circ [0, \mathbf{z}', ..., \mathbf{z}^{(r)}] \\
&= \frac{1}{p}[l^{\phi^r}] \circ [\Phi^{\phi^r}] \circ [\phi^r(\mathbf{z})] \circ [0, \mathbf{z}', ..., \mathbf{z}^{(r)}] \\
&= \frac{1}{p}[z_1 + z_2] \circ [l^{\phi^r}] \circ [\phi^r(\mathbf{z})] \circ [0, \mathbf{z}', ..., \mathbf{z}^{(r)}] \\
&= L_p^r(z_1', ..., z_1^{(r)}) + L_p^r(z_2', ..., z_2^{(r)}).
\end{aligned}$$

□

5.3. Here is one more remark that will be useful later. Assume we are in the global case. Let Φ, l, and e be a commutative formal group law over M in g variables, its logarithm, and its exponential, respectively. We claim that, for each $p \notin S$, $p^{-1}e(pz)$ belongs to $(M[z]^{\wedge p})^g$ and that

$$(p^{-1}e(pz)) \in \prod_{p \notin S} (M[z]^{\wedge p})^g$$

are Fermat with respect to the standard Fermat structure. Indeed, by the proof of Proposition 5.1, we can write

$$p^{-1}l(pz) = z + ph_p(z),$$

where

$$(h_p(z)) \in \prod_{p \notin S} (M[z]^{\wedge p})^g$$

are Fermat. Now $(p^{-1}e(pz))$ is the $\mathbf{p}-$adic limit of the sequence

$$(e_p^{(\nu)}(z)) \in \prod_{p \notin S} (M[z]^{\wedge p})^g$$

defined inductively by $e_p^{(0)}(z) := z$ and

$$e_p^{(\nu+1)}(z) := z - h_p(e_p^{(\nu)}(z))$$

which immediately implies our claim.

6. Differential characters and differential modular forms

The plan of this section is the following. We will first review some of the results in [5], [7] on differential characters, and results in [8], [1], [2] on (Siegel) differential modular forms. Next we will give two constructions, a crystalline one and a $p-$jet theoretical one of Siegel differential modular forms which we call $f_{cris,p}^n$ and $f_{jet,p}^n$, respectively. Due to a "multiplicity one theorem" in [2] which we shall recall here these forms are "proportional". On the other hand it turns out (easy) that $f_{cris,p}^n$ for $n = 1, 2$ contain all relevant information as to the crystalline cohomology of our

Abelian schemes while (and this is harder to see) $f^n_{jet,p}$ form Fermat families. The above facts can then be easily combined to conclude the proof of the conjecture for curves and Abelian varieties. Note that we will defer to Section 7 the verification of the fact that the construction we give here for $f^n_{jet,p}$ indeed leads to a Siegel differential modular form with the desired properties for each fixed p. The verification that $f^n_{jet,p}$, as p varies, form a Fermat family will be deferred to Section 8.

6.1. **δ-characters ([5], [7]).** Start with a prime integer $p \neq 2, 3$ and let $R \in \mathbf{Witt}_p$ have an algebraically closed field. Recall that there is a canonical operator $\delta : R \to R$ defined by the formula $\delta x := (\phi(x) - x^p)/p$, $x \in R$, and call $\delta x, \delta^2 x, ...$ the *$p-$derivatives* of order $1, 2, ...$ of x. Let G_R be a smooth commutative group scheme over R. In [5] we introduced the notion of *$\delta-$character* of G_R *of order* $\leq r$; by definition this means a group homomorphism $\psi : G_R(R) \to R$ that can be represented, on each of the sets of an affine open Zariski cover, as a $p-$adic limit of polynomials with $R-$coefficients in the affine coordinates and their $p-$derivatives up to order r. Any such $\delta-$character is induced by a unique homomorphism $J^r(G_R{}^{\hat{}p}) \to \mathbf{G}_{a,R}{}^{\hat{}p}$ in $\mathbf{FSch}_R$, where $\mathbf{G}_{a,R}{}^{\hat{}p} := Spf\ R[x]^{\hat{}p}$ is the $p-$adic completion of the additive group over R. By abuse we also write $\psi : G_R \to \mathbf{G}_a$.

Let us assume now $G_R = E_R$ is an elliptic curve (i.e. an Abelian scheme of relative dimension one) over R.

By [5], Proposition (3.2), there exists a non-zero $\delta-$character $\psi : E_R \to \mathbf{G}_a$ of order ≤ 2; moreover there exists a $\delta-$character of order 1 if and only if the $p-$th power Frobenius of the closed fiber E_k lifts to a $\phi-$linear endomorphism of E_R. Assume ψ above has minimum possible order. Then by [5], (2.10), ψ is uniquely determined up to multiplication by an element in the quotient field of R. Let ω be a generator of the $R-$module of invariant $1-$forms on E_R. Then by [5], (2.9), we have the following local expression for ψ around the origin:

$$\psi(P) = \Lambda_\psi(p^{-1} \cdot log_\omega P), \quad P \in E_R(pR), \tag{6.1}$$

for a unique $\Lambda_\psi = \lambda_2\phi^2 + \lambda_1\phi + \lambda_0 \in R[\phi]$, where $E_R(pR)$ is the kernel of the reduction map $E_R(R) \to E_k(k)$ and $log_\omega : E_R(pR) \to pR$ is the formal logarithm map associated to ω. In [5] Λ_ψ was called the Picard-Fuchs operator associated to ψ. Actually by [5], (3.2), (3.3), (4.5), one can choose ψ such that either $\lambda_2 = 1$, or $\lambda_2 = 0$ and $\lambda_1 = 1$. If this holds, then we shall say ψ is *normalized* with respect to ω. Such a normalized ψ is uniquely determined by the pair (E_R, ω).

More generally, if $G_R = E_R$ is an Abelian scheme of relative dimension $g \geq 1$ over R, ψ is a $g-$tuple of $\delta-$characters $E_R \to \mathbf{G}_a$ of order ≤ 2 and ω is an $R-$basis for the module of $1-$forms on E_R, then, by the theory in [5], the formula (6.1) holds again for a unique operator

$$\Lambda_\psi = \lambda_0\phi^2 + \lambda_1\phi + \lambda_0, \quad \lambda_0, \lambda_1, \lambda_2 \in gl_g(R).$$

(Here, for any ring A we denote by $gl_g(A)$ the set of all $g \times g$ matrices with coefficients in A.) The operator Λ_ψ will be called, again, the *Picard-Fuchs operator* associated to ψ.

Going back to the one-dimensional case define the following set:

$$\mathbf{M}(R) = \{(a, b) \in R^2; \Delta(a, b) \in R^\times\},$$

where $\Delta(a, b) := 4a^3 + 27b^2$.

Assume $E_R = E_{a,b}$ is an elliptic curve in Weierstrass form $y^2 = x^3 + ax + b$ with $(a, b) \in \mathbf{M}(R)$. Then we set $\Lambda_{a,b} := \Lambda_\psi$, where ψ is the unique normalized $\delta-$character associated to the pair $(E, dx/y)$.

The following was proved in [7], Theorem (1.10), and will be used later:

Theorem 6.1 ([7])**.** *Assume $a, b \in \mathbf{Z}_p$ and let $E_{\mathbf{Z}_p}$ be the elliptic curve over $\mathbf{Z}_p$ corresponding to (a, b). Assume the $p-$power Frobenius on $E_{\mathbf{Z}_p} \otimes \mathbf{F}_p$ does not lift to an endomorphism of $E_{\mathbf{Z}_p}$. Then $\Lambda_{a,b} = \phi^2 - \tau_p \phi + p$, where τ_p is the trace of the $p-$power Frobenius on $E_{\mathbf{Z}_p} \otimes \mathbf{F}_p$.*

We need the following complement to the above theorem.

Theorem 6.2. *Assume $R \in \mathbf{Witt}_p$ has finite residue field k of size p^d and let $(a, b) \in \mathbf{M}(R)$ be such that the elliptic curve E_R corresponding to (a, b) has ordinary reduction. Assume the $p-$power Frobenius on $E_k := E_R \otimes k$ lifts to an endomorphism of E_R. Then $\Lambda_{a,b} = \phi - pu$, $u \in R$, and the characteristic polynomial of the p^d power Frobenius acting on E_k coincides with the characteristic polynomial of the matrix $\phi^{d-1}\gamma \cdots \phi\gamma \cdot \gamma$, where*

$$\gamma = \begin{bmatrix} 1/u & 0 \\ 0 & pu \end{bmatrix}.$$

Proof. The case $d = 1$ was proved in [7]. The general case can be proved in a similar way. Indeed, if $l(z) \in R[1/p][[z]]$ is the logarithm of the formal group of E_R, then, exactly as in [7], we get

$$l^\phi(z^p) - pu \cdot l(z) \in pR[[z]].$$

By induction one gets, for all i,

$$l^{\phi^i}(z^{p^i}) - p^i \phi^{i-1} u \cdots \phi u \cdot u \cdot l(z) \in pR[[z]].$$

In particular, for $i = d$ we have $l^{\phi^d}(z) = l(z)$ and $v := \phi^{d-1} u \cdots \phi u \cdot u \in \mathbf{Z}_p$. As in [7] we obtain that the p^d power Frobenius of the formal group of E_R is just the multiplication $[p^d v]$ on the Formal group. But on the other hand the p^d power Frobenius on the formal group must be a root of $x^2 - \tau x + p^d$, where τ is the trace of the p^d power Frobenius on E_k. In particular $p^d v$ and v^{-1} are the roots of the above quadratic polynomial and the conclusion follows. □

6.2. **Siegel δ-modular forms (**[2]**).** For any Noetherian ring S we let $\mathbf{M}_g(S)$ denote the set of all triples (E, θ, ω), where E/S is an Abelian scheme of relative dimension g, $\theta : E \to \check{E}$ is a principal polarization, and $\omega = (\omega_1, ..., \omega_g)^t$ is a column vector whose entries are a basis of the $S-$module of $1-$forms $H^0(E, \Omega^1_{E/S})$; so the latter is supposed, by our very definition, to be free. (Also $\mathbf{M}_1(R)$ coincides with the set $\mathbf{M}(R)$ defined previously.)

By a *Siegel $\delta-$modular function* of genus g, size m, and order $\leq n$ we understand a rule, call it f, that associates to any prolongation sequence $S^* \in \mathbf{Prol}_p$ and to any triple $(E, \theta, \omega) \in \mathbf{M}_g(S^0)$ an $m \times m$ matrix

$$f(E, \theta, \omega, S^*) \in gl_m(S^n)$$

satisfying the following properties:

6.2.1. $f(E, \theta, \omega, S^*)$ depends on S^* and the isomorphism class of (E, θ, ω) only.

6.2.2. The formation of $f(E,\theta,\omega,S^*)$ is functorial in S^* in the sense that if $\pi : S^* \to \tilde{S}^*$ is a morphism of prolongation sequences in $\mathbf{Prol}_p$ and π^* denotes "pull back via π", then

$$f(\pi^*E,\pi^*\theta,\pi^*\omega,\tilde{S}^*) = \pi(f(E,\theta,\omega,S^*)).$$

Sometimes, when no confusion arises, we will write $f(E,\theta,\omega)$ in place of $f(E,\theta,\omega,S^*)$.

Let G and G' be group schemes over $\mathbf{Z}_p$. By a *$\delta-$homomorphism* $\chi : G \to G'$ of order $\leq n$ we mean a rule that associates to any prolongation sequence $S^* \in \mathbf{Prol}_p$ a group homomorphism

$$\chi : G(S^0) \to G'(S^n)$$

which is "functorial in S^*" in the obvious sense. By a *Siegel $\delta-$weight* of genus g, size m, and order $\leq n$ we mean a pair (χ_l,χ_r) of $\delta-$homomorphisms of order $\leq n$:

$$\chi_l,\chi_r : GL_g \to GL_m,$$

each of them commuting with transposition of matrices $\gamma \mapsto \gamma^t$. (The indices l and r stand here for "left" and "right".) Examples of Siegel $\delta-$weights of size g that will play a role later are pairs (ϕ^a,ϕ^b), where

$$\phi^a : GL_g(S^0) \to GL_g(S^a)$$

are induced by the iterates a times of the ring homomorphisms $\phi : S^i \to S^{i+1}$, $\phi(x) = x^p + p\delta x$. A Siegel $\delta-$modular function f as above will be called a *Siegel $\delta-$modular form* of Siegel $\delta-$weight (χ_l,χ_r) if the following condition is satisfied:

6.2.3. The formation of $f(E,\theta,\omega,S^*)$ has the following covariance with respect to ω; if $(E,\theta,\omega) \in \mathbf{M}_g(S^0)$ and $\lambda \in GL_g(S^0)$, then

$$f(E,\theta,\lambda\omega,S^*) = \chi_l(\lambda)\cdot f(E,\theta,\omega,S^*)\cdot\chi_r(\lambda^t).$$

To introduce our next concept we need more notation. Let

$$(E_1,\theta_1,\omega_1),(E_2,\theta_2,\omega_2) \in \mathbf{M}_g(S)$$

and let $u : E_1 \to E_2$ be an isogeny (which is not assumed to be compatible with the forms or the polarizations). We let

$$u^t := \theta_1^{-1}\circ\check{u}\circ\theta_2 : E_2 \to \check{E}_2 \to \check{E}_1 \to E_1$$

denote its transpose and we let $[u]$ be the unique $g\times g$ matrix with $S-$coefficients such that $u^*\omega_2 = [u]\cdot\omega_1$. (Recall that $u^{tt} = u$. Also recall that $[u^t] \neq [u]^t$ in general. Moreover, it is easy to check that $deg(u)^2 = det([u\circ u^t])^2 = det([u])^2\cdot det([u^t])^2$. Hence, if S is a $\mathbf{Z}_p-$algebra, then $deg(u)$ is prime to p if and only if u and $\check{u}$ are etale; in this case, $[u],[u^t] \in GL_g(S)$.)

A Siegel $\delta-$modular form of weight (χ_l,χ_r) will be called *isogeny covariant* if the following condition holds:

6.2.4. For any prolongation sequence $S^* \in \mathbf{Prol}_p$, any $(E_1,\theta_1,\omega_1),(E_2,\theta_2,\omega_2) \in \mathbf{M}_g(S^0)$, and any isogeny $u : E_1 \to E_2$, of degree prime to p, such that $[u]$ is the identity (i.e. such that $u^*\omega_2 = \omega_1$), the following equality holds:

$$f(E_1,\theta_1,\omega_1,S^*) = f(E_2,\theta_2,\omega_2,S^*)\cdot\chi_r([u^t]^t).$$

We denote by $I_g^n(\chi_l,\chi_r)$ the space of all isogeny covariant Siegel $\delta-$modular forms of Siegel $\delta-$weight (χ_l,χ_r). Our definition of Siegel $\delta-$modular forms here

agrees with the one for $g = 1$ given in [8], [2]. Note that a Siegel $\delta-$modular form of genus $g = 1$, size $m = 1$, order $\leq r$ and Siegel $\delta-$weight (χ_l, χ_r) in the sense of the present paper is the same as a $\delta-$modular form of weight $\chi_l^{-1}\chi_r^{-1}$: $\lambda \mapsto \chi_l(\lambda)^{-1}\chi_r(\lambda)^{-1}$ in the sense of [8]. (Note the exponent -1!) However the definition of isogeny covariance in the present paper is slightly different from that given in [8]: instead of asking, as here, that the isogenies under consideration have order prime to p, we only asked in [8] that these isogenies be etale. Nevertheless all results stated in [8] continue to hold true, with identical proofs, if the definition of isogeny covariance given there is replaced by the definition given here.

We will need the following result proved in [2]:

Theorem 6.3 ([2])**.** *The $\mathbf{Z}_p-$module $I_g^n(\phi^r, \phi^s)$ has rank one if $n \geq r$, $n \geq s$, $r \neq s$, and has rank zero in all other cases.*

It is also useful to keep in mind that, in case $g = 1$, a (Siegel) $\delta-$modular function (of size one) is simply an element f of the ring

$$\mathbf{Z}_p[a_4, a_6, a_4', a_6', ..., a_4^{(r)}, a_6^{(r)}, \Delta^{-1}]^{\wedge p},$$

where $a_4, a_6, a_4', a_6', ..., a_4^{(r)}, a_6^{(r)}$ are variables and $\Delta = 4a_4^3 + 27a_6^2$; for $(a, b) \in \mathbf{M}(R)$ we shall use the notation

$$f\langle a, b\rangle = f(a, b, \delta a, \delta b, ..., \delta^r a, \delta^r b, \Delta^{-1}).$$

Let us end the discussion here by introducing more notations that will be needed later. Assume we are given $M^* \in \mathbf{Prol}_p$ and $(E, \theta, \omega) \in \mathbf{M}_g(B)$, where $B = Spec\, M^0$. Then we let $\bar{B} = B \otimes (R/pR)$, $\bar{M}^0 = \mathcal{O}(\bar{B})$, $\bar{M}^r = M^r/pM^r$, $\bar{E} = E \otimes_B \bar{B}$, and for a Siegel $\delta-$modular form f of size g we let $\bar{f}(E, \theta, \omega, M^*) \in gl_g(\bar{M}^r)$ be the image of $f(E, \theta, \omega, M^*)$. Now, the polarization $\theta : E \to \check{E}$ induces an isomorphism $\theta_* : H^0(E, T_{E/B}) \to H^1(E, \mathcal{O})$ at the level of Lie algebras, so if v is the basis of $H^0(E, T_{E/B})$ dual to ω (we view v as a column vector), then $u = \theta_* v$ is a basis of $H^1(E, \mathcal{O})$. We get an induced basis $\bar{u}$ of $H^1(\bar{E}, \mathcal{O})$. Then we can consider the Hasse-Witt matrix $\bar{H} \in gl_g(\bar{M}^0)$ of $\bar{E}/\bar{B}$ corresponding to the basis $\bar{u}$; by definition this is the matrix, with respect to $\bar{u}$, of the semilinear map induced by the $p-$power Frobenius

$$F^* : H^1(\bar{E}, \mathcal{O}) \to H^1(\bar{E}, \mathcal{O});$$

i.e. $F^*\bar{u} = \bar{H} \cdot \bar{u}$. Note that $\bar{H} = \bar{H}(\bar{E}, \bar{\theta}, \bar{\omega})$ is naturally associated to the reduction mod p of (E, θ, ω).

6.3. **Crystalline construction.** Let us recall from [2] how, for each p, one can construct, using crystalline cohomology, a sequence of non-zero Siegel $\delta-$modular forms $f_{crys,p}^n \in I_g^n(\phi^n, \phi^0)$, $n \geq 1$. The construction is done for any g and will be compatible, in the obvious sense, with products of principally polarized schemes.

Let $S^* \in \mathbf{Prol}_p$, $(A, \theta, \omega) \in \mathbf{M}_g(S^0)$, and let $H := H_{DR}^1(E/S^0)$ be the first DeRham module of E/S^0. Crystalline theory provides $\phi-$linear maps:

$$\Phi : H \otimes S^i \to H \otimes S^{i+1}$$

(tensor products being taken over S^0). We also have a canonical exact sequence

$$0 \to H^0(E, \Omega_{E/S^0}^1) \xrightarrow{\alpha} H_{DR}^1(E/S^0) \xrightarrow{\beta} H^1(E, \mathcal{O}) \to 0$$

inducing analogue exact sequences over any S^i; we shall still denote by α, β the corresponding morphisms; we shall view all morphisms α as inclusions. We have

$$\Phi H^0(E, \Omega^1_{E/S^0}) \subset p \cdot H \otimes S^1.$$

We may consider the elements

$$p^{-1}\Phi^n \omega_i \in H \otimes S^n,$$

and their projections

$$\beta p^{-1}\Phi^n \omega_i \in H^1(E, \mathcal{O}) \otimes S^n.$$

The principal polarization $\theta : E \to \check{E}$ induces an S^0-linear isomorphism at the level of Lie algebras

$$\theta_* : H^0(E, T_{E/S^0}) \to H^1(E, \mathcal{O}).$$

We shall still denote by θ_* the tensor product $\theta_* \otimes S^n$. Then we can consider the inverse image

$$\theta_*^{-1}\beta p^{-1}\Phi^n \omega_i \in H^0(E, T_{E/S^0}) \otimes S^n$$

and pair it with ω_j (under the natural pairing between the tangent sheaf T and the cotangent sheaf Ω^1) to get a $g \times g$ matrix with entries

$$\langle \theta_*^{-1}\beta p^{-1}\Phi^n \omega_i, \omega_j \rangle \in S^n.$$

This matrix is, by definition, our

$$f^n_{crys,p}(E, \theta, \omega, S^*) \in gl_g(S^n).$$

It is easy to check that f^n_{crys} is indeed an element of $I^n_g(\phi^n, \phi^0)$.

Another way to express the definition of f^n_{cris} is the following. Let $\check{H} := H^1_{DR}(\check{E}/S^0)$. By [12], p. 81, there is a canonical bilinear pairing

$$\langle\ ,\ \rangle : \check{H} \times H \to S^0$$

induced by the Poincare bundle. Now θ defines an isomorphism $\theta_{DR} : \check{H} \to H$. Define

$$\langle\ ,\ \rangle_\theta : H \times H \to S^0$$

by the equation

$$\langle \eta_1, \eta_2 \rangle_\theta := \langle \theta^{-1}_{DR}\eta_1, \eta_2 \rangle.$$

The pairing $\langle\ ,\ \rangle_\theta$ is perfect, antisymmetric, and $H^0(E, \Omega^1)$ is an isotropic subspace. It induces a paring, still denoted by

$$\langle\ ,\ \rangle_\theta : (H \otimes S^n) \times (H \otimes S^n) \to S^n.$$

One immediately checks that

$$f^n_{crys,p}(E, \theta, \omega, S^*) = p^{-1}\langle \Phi^n \omega, \omega^t \rangle_\theta.$$

By the way, if $E = Jac(X)$ is the Jacobian of a (smooth projective) curve X/S^0, S^0 an integral domain, and θ is induced by the theta divisor, then, under the identification $H \simeq H^1_{DR}(X/S^0)$ given by the Abel-Jacobi map, the pairing $\langle\ ,\ \rangle_\theta : H \times H \to S^0$ corresponds to the Poincare duality paring

$$\langle\ ,\ \rangle : H^1_{DR}(X/S^0) \times H^1_{DR}(X/S^0) \to S^0;$$

one can see this, for instance using the analytic picture in [13], pp. 326-328. So if $E = Jac(X)$, θ is the polarization induced from the theta divisor, and S^* is the

prolongation sequence associated to $R \in \mathbf{Witt}_p$, then we have

$$\langle \Phi\eta', \Phi\eta'' \rangle_\theta = p \cdot \phi(\langle \eta', \eta'' \rangle_\theta) \tag{6.2}$$

for all $\eta', \eta'' \in H^1_{DR}(E/R)$; this is because the same holds for the Poicare duality on X [11], p. 118. More generally, let us say that a principally polarized Abelian scheme (E, θ) over a ring S is *complementable* if there exists a principally polarized Abelian scheme (E', θ') over S and an isogeny of degree prime to p from $E \times E'$ into a Jacobian of a curve over S. The isogeny is assumed, as usual, to be defined over S and, as usual, is not required to preserve polarizations. Then it is trivial to check, using the information on Jacobians, that (6.2) holds for all $\eta', \eta'' \in H^1_{DR}(E/R)$ whenever (E, θ) is complementable.

Finally, let us record the following easy fact that will play a key role later.

Lemma 6.4. *Let $R \in \mathbf{Witt}_p$, let $(E, \theta, \omega) \in \mathbf{M}_g(R)$, and assume (E, θ) is complementable. Set $f^i_{cris} := f^i_{cris,p}(E, \theta, \omega) \in R$, $i = 1, 2$, and assume $\det f^1_{cris} \in R^\times$. Then $(\omega^t, \Phi\omega^t)$ is a basis for $H = H^1_{DR}(E/R)$ and the matrix of $\Phi : H \to H$ with respect to this basis is*

$$\begin{bmatrix} 0 & I \\ M & N \end{bmatrix}, \tag{6.3}$$

where

$$M = \phi(f^1_{cris}) \cdot ((f^1_{cris})^t)^{-1}, \quad N = f^2_{cris} \cdot (f^1_{cris})^{-1}.$$

Proof. The matrix of $\Phi : H \to H$ has the form (6.3) with M, N satisfying

$$\Phi^2\omega = M \cdot \omega + N \cdot \Phi\omega. \tag{6.4}$$

Taking $\langle\ , \omega^t\rangle_\theta$ and $\langle\ , \Phi\omega\rangle_\theta$ in (6.4) and using the antisymmetry of $\langle\ ,\ \rangle_\theta$ as well as its compatibility with Φ we derive the desired expressions for M and N. □

6.4. **Jet construction.** In this section we construct, for any $R \in \mathbf{Witt}_p$, a sequence of maps

$$f^r_{jet,p} : \mathbf{M}_g(R) \to R. \tag{6.5}$$

Theorem 6.6 below will say, in particular, that these maps "extend" (uniquely) to Siegel $\delta-$modular forms $f^r_{jet,p} \in I^r_g(\phi^r, \phi^0)$.

Let $(E, \theta, \omega) \in \mathbf{M}_g(R)$. Consider the projection $\pi : J^r(E^{\wedge p}) \to E^{\wedge p}$ and let N_p be the kernel of π. Then N_p can be identified with the ($p-$adic completion of the) affine space of dimension rg over R. Now π locally has sections so it induces a $1-$cocycle on $E^{\wedge p}$ with values in the sheaf of N_p-valued functions. We can consider the group homomorphism $N_p \to (\mathbf{G}_a^g)^{\wedge p}$ induced by the series L^r_p constructed in Section 5; the image of our cocycle via this homomorphism defines a vector of cohomology classes in $H^1(E, \mathcal{O})$. Using the polarization θ one can pull back these classes to the Lie algebra $H^0(E, T_{E/R})$ and one can pair the result with ω to get a matrix $f^r_{jet,p}(E, \theta, \omega) \in gl_g(R)$. (More details on this construction will be given in Section 7.)

For $g = 1$ it is known from [8] that the maps (6.5) extend to $\delta-$modular forms $f^r_{jet,p} \in I^r_1(\phi^r, \phi^0)$; if we view $f^1_{jet,p}$ as an element of $\mathbf{Z}_p[a_4, a_6, a'_4, a'_6, \Delta^{-1}]^{\wedge p}$, then its reduction mod p, viewed as an element $\bar{f}^1_{jet,p} \in \mathbf{F}_p[a_4, a_6, a'_4, a'_6, \Delta^{-1}]$, was computed explicitly by C. Hurlburt [15] in the following theorem.

Theorem 6.5 ([15])**.**

$$\bar{f}^1_{jet,p} = \bar{c}\bar{E}_{p-1}\bar{\Delta}^{-p}(2a_4^p a_6' - 3a_6^p a_4') + \bar{f}_0,$$

where $c \in \mathbf{Z}_p^\times$, $\bar{E}_{p-1} \in \mathbf{F}_p[a_4, a_6]$ *is the reduction mod* p *of the normalized Eisenstein form of weight* $p-1$ *(the Hasse invariant) and* $\bar{f}_0 \in \mathbf{F}_p[a_4, a_6, \Delta^{-1}]$*, with* $\bar{\Delta}^p \bar{f}_0 \in \mathbf{F}_p[a_4, a_6]$ *a polynomial of weight* $11p-1$.

For arbitrary g the following theorem will be proved in section 7:

Theorem 6.6. *The maps* (6.5) *extend uniquely to Siegel* $\delta-$*modular forms* $f^r_{jet,p} \in I^r_g(\phi^r, \phi^0)$ *satisfying the following properties:*

1. *For each* r *and variable* g*, the forms* $f^r_{jet,p}$ *are compatible with products of principally polarized Abelian schemes.*

2. *If* $R \in \mathbf{Witt}_p$ *and* $(E, \theta, \omega) \in \mathbf{M}_g(R)$*, then* $f^1_{jet,p}(E, \theta, \omega) = 0$ *if and only if the* $p-$*power Frobenius of* $E \otimes (R/pR)$ *lifts to* E*. (By a lifting to* E *we mean, of course, a* $\phi-$*linear lifting.)*

3. *If* $R \in \mathbf{Witt}_p$ *and* $(E, \theta, \omega) \in \mathbf{M}_g(R)$ *is such that*

$$\det(f^1_{jet,p}(E, \theta, \omega)) \in R^\times,$$

then there exists a (unique) $g-$*tuple of* $\delta-$*characters of* E *of order* ≤ 2 *whose Picard-Fuchs operator has the form*

$$\phi^2 - f^2_{jet,p}(E, \theta, \omega)[f^1_{jet,p}(E, \theta, \omega)]^{-1}\phi + h$$

for some $h \in gl_g(R)$.

4. *Let* $M^* \in \mathbf{Prol}_p$*,* $B = Spec\ M^0$*,* $(E, \theta, \omega) \in \mathbf{M}_g(B)$ *and let* $\bar{H} = \bar{H}(\bar{E}, \bar{\theta}, \bar{\omega})$ *be the associated Hasse-Witt matrix. Then*

$$\bar{f}^r_{jet,p}(E, \theta, \omega, M^*) = (\bar{f}^1_{jet,p}(E, \theta, \omega, M^*))^{F^{r-1}} \cdot \bar{H}^{F^{r-2}} \cdots \bar{H}^F \cdot \bar{H}.$$

The upper F here means, of course, the image under the $p-$power Frobenius.

A by-product of our theory will be the following strengthening of one of our main results in [5]; the theorem below plays a key role in our paper [9] where we prove what we call an "infinitesimal Lang-Mordell" theorem.

Theorem 6.7. *Let* $R \in \mathbf{Witt}_p$ *and let* $(E, \theta, \omega) \in \mathbf{M}_g(R)$*,* E/R *with ordinary reduction mod* p*. Let* $q_{ij}(E) \in 1 + pR$ *be the Serre-Tate parameters of* E*,* $1 \leq i, j \leq g$*, and assume* $\det((q_{ij}(E) - 1)/p) \in R^\times$*. Then* $det\ f^1_{jet,p}(E, \theta, \omega) \in R^\times$*. Moreover there exists a* $g-$*tuple of* $\delta-$*characters of* E *of order* ≤ 2 *whose Picard-Fuchs operator has the form* $\phi^2 + \lambda_1\phi + \lambda_0$*, with* $\det \lambda_1 \in R^\times$.

This will be used in conjunction to the following easy lemma which was proved in [9]:

Lemma 6.8 ([9])**.** *Let* $W \in \mathbf{Witt}_p$ *have an algebraically closed residue field* k *and set* $R_2 = R/p^2R$*. Assume* C_k/k *is an ordinary, non-hyperelliptic curve of genus* g *and let* $Def(C_k, R_2)$ *be the set of isomorphism classes of liftings of* C_k *to* R_2 *(the latter has a structure of affine space over* k*). Then there exists a dense Zariski open set* $V \subset Def(C_k, R_2)$ *such that any curve* C/R *whose reduction mod* p^2 *belongs to* V *has the property that its Jacobian has Serre-Tate parameters* $q_{ij} \in 1 + pR$ *with*

$$\det((q_{ij} - 1)/p) \in R^\times.$$

One more notation is needed for the statement of the following theorem. Assume $B = Spec\ M$ is a smooth affine scheme over $\mathbf{Z}$. Let $M_p^r := \mathcal{O}(J^r(B^{\wedge p}))$; so in particular $M_p^0 = M^{\wedge p}$. For each p we have a prolongation sequence $M_p^* \in \mathbf{Prol}_p$. Then for any $(E, \theta, \omega) \in \mathbf{M}_g(B)$ and any prime p, which is not invertible on B, we denote by $f_p^r(E, \theta, \omega)$ the matrix

$$f_p^r(E \otimes M_p^0, \theta \otimes M_p^0, \omega \otimes M_p^0, M_p^*) \in gl_m(M_p^r) = gl_m(\mathcal{O}(J^r(B^{\wedge p}))).$$

The following theorem will be proved in Section 8:

Theorem 6.9. *The forms $f_{jet,p}^r$ in Theorem 6.6 have, in addition, the following property. For any smooth affine scheme $B/\mathbf{Z}$ and any $(E, \theta, \omega) \in \mathbf{M}_g(B)$ there exists a finite set of primes S and a dense affine Zariski open set B' of B such that the image of the family*

$$(f_{jet,p}^r(E, \theta, \omega)) \in \prod_{p \notin S} gl_g(\mathcal{O}(J^r(B^{\wedge p})))$$

in the product

$$\prod_{p \notin S} gl_g(\mathcal{O}(J^r(B'^{\wedge p})))$$

is Fermat.

Remark 6.10. In order to prove Theorem 6.9, it is enough to prove a weaker version of it obtained by replacing, in its statement, the words "Zariski open set" by "etale open set" and the word "Fermat" by the words "formally Fermat". Indeed assume we have proved this weaker version. By Proposition 4.1 we may assume that we have an isomorphism of families with Fermat structure $(\mathcal{O}(J^r(B^{\wedge p}))) \simeq (\mathcal{O}(B)[t]^{\wedge p})$ and $(\mathcal{O}(J^r(B'^{\wedge p}))) \simeq (\mathcal{O}(B')[t]^{\wedge p})$ for some indeterminates t. But then Theorem 6.9 follows from its weaker version via Proposition 3.10.

In case $g = 1$ we will prove a more precise statement:

Theorem 6.11. *Assume that $g = 1$. Then there exists a finite set of primes S such that if N is the product of the primes in S, $B = \mathbf{Z}[1/N][a_4, a_6, \Delta^{-1}]$, and (E, θ, ω) is the standard elliptic curve in Weierstrass form over B, then the family*

$$(f_{jet,p}^r(E, \theta, \omega)) \in \prod_{p \notin S} \mathbf{Z}_p[a_4, a_6, a_4', a_6', ..., a_4^{(r)}, a_6^{(r)}, \Delta^{-1}]^{\wedge p}$$

is Fermat.

For the Conjecture in the CM case we will need:

Theorem 6.12. *There exists a finite set of primes S and a Fermat family*

$$k = (k_p) \in \prod_{p \notin S} \mathbf{Z}_p[a_4, a_6, a_4', a_6', \Delta^{-1}]^{\wedge p}$$

such that for any $R \in \mathbf{Witt}_p$ and any $(a, b) \in M(R)$ the following holds:

$$if \quad f_{jet}^1\langle a, b\rangle = 0, \quad then \quad \Lambda_{a,b} = \phi - pk\langle a, b\rangle.$$

6.5. **Proof of Theorems 2.2, 2.3, 2.4, 2.5.**

6.5.1. Let us start by proving Theorem 2.5.

Proof. Let j_0 be the $j-$invariant of the geometric generic fiber of X/Y. This fiber has complex multiplication by $\mathcal{O}_{K_0}$ (i.e. its endomorphism ring is $\mathcal{O}_{K_0}$; for the terminology of complex multiplication we are using, we refer to [25]). In particular $j_0 \in \bar{\mathbf{Q}}$. By [25], p. 122, we must have $K_0 \not\subset \mathbf{Q}(j_0)$. Note that, due to the presence of the invertible $1-$form on X, we can write a Weierstrass equation for X with coefficients in $\mathcal{O}(Y)$. In particular $j_0 \in \mathcal{O}(Y)$. Now let $\mathcal{E}$ be an elliptic curve over $\mathbf{Q}(j_0)$ with $j-$invariant j_0. Then $\mathcal{E}$ has complex multiplication by $\mathcal{O}_{K_0}$ (i.e. its endomorphism ring over $\bar{\mathbf{Q}}$ is $\mathcal{O}_{K_0}$). By [25], p. 184, for any place of $\mathbf{Q}(j_0)$ that splits in $K = K_0(j_0)$, the reduction of $\mathcal{E}$ at that place is ordinary. In particular there is a finite set S of primes such that:

Fact 1. If $p \notin S$ splits completely in K, then the reduction of $\mathcal{E}$ at any place above p is ordinary.

Upon enlarging S we claim the following is true:

Fact 2. For any a closed point $y \in Y$ of characteristic p with p splitting completely in K, the reduced elliptic curve X_y is ordinary.

Indeed, if v is the place of $\mathcal{O}_{\mathbf{Q}(j_0)}$ corresponding to the map

$$\mathcal{O}_{\mathbf{Q}(j_0)} \subset \mathcal{O}(Y) \to \kappa(y),$$

then, by Fact 1, the image of j_0 in the residue field of $\mathcal{O}_{\mathbf{Q}(j_0)}$ at v is an ordinary $j-$invariant. But then X_y, having the same $j-$invariant, is ordinary.

Next let $R \in \mathbf{Witt}_p$ and $P \in Y(R)_!$ be such that p splits completely in K and let X_P be the elliptic curve over R, pull back of X via P. Let $k = R/pR$ and $X_k = X_P \otimes k$. Then, by Fact 2 above, $X_k = X_{y(P)}$ is ordinary, hence its endomorphism ring $End_k(X_k)$ is an order in the ring of integers of an imaginary quadratic extension of the rationals [24], p. 102 and p. 137. Then the composition

$$\mathcal{O}_{K_0} \to End_R(X_R) \to End_k(X_k)$$

must be an isomorphism. In particular the second arrow above is an isomorphism. Since k is finite, by [19], pp. 177-178, it follows that the $p-$power Frobenius on X_k lifts to X_R. By assertion 2) in Theorem 6.6 $f^1_{jet}\langle P\rangle = 0$. (Here we take for coordinates of P the corresponding coefficients of the Weierstrass equation). By Theorems 6.2 and 6.12 the characteristic polynomial of the $N(y)-$power Frobenius on X_y coincides with the characteristic polynomial of the matrix $\phi^{d-1}\gamma \cdots \phi\gamma \cdot \gamma$ where

$$\gamma = \begin{bmatrix} 1/k\langle P\rangle & 0 \\ 0 & p \cdot k\langle P\rangle \end{bmatrix},$$

where k is the Fermat adele in Theorem 6.12. This concludes the proof of part 2) of the Conjecture in the case of Theorem 2.5. Part 1) of the Conjecture follows immediately. □

6.6. To prove the rest of the theorems we proceed by proving a series of lemmas.

Lemma 6.13. *For any p there exists a pair $(a, b) \in \mathbf{M}(\mathbf{Z}_p)$ such that*

$$f^1_{jet}\langle a, b\rangle \in \mathbf{Z}_p^\times.$$

Proof. This follows immediately, for instance, from Hurlburt's formula (Theorem 6.5): if one takes two pairs (a,b) and (α,β) of integers such that $\alpha = a + pn$ and $\beta = b + pm$, then the difference

$$f^1_{jet}\langle \alpha,\beta\rangle - f^1_{jet}\langle a,b\rangle$$

divided out by $\bar{c}$ equals the reduction mod p of

$$E_{p-1}(a,b)\Delta(a,b)^{p-1}(2am - 3bn).$$

We conclude by choosing (a,b) such that $E_{a,b}$ is ordinary, and varying m,n. □

Lemma 6.14. *For each p there exists $c_p \in \mathbf{Z}_p^\times$, such that*

$$f^i_{cris,p} = c_p \cdot f^i_{jet,p} \in I^i_g(\phi^i,\phi^0)$$

for $i = 1,2$.

Proof. By Theorem 6.3 there exist $c^1_p, c^2_p \in \mathbf{Z}_p$ such that

$$f^i_{cris,p} = c^i_p \cdot f^i_{jet,p} \in I^i_g(\phi^i,\phi^0) \tag{6.6}$$

for $i = 1,2$. So it is enough to show that $c^1_p \in \mathbf{Z}_p^\times$ and $c^1_p = c^2_p$. Indeed we cannot have $c^1_p \in p\mathbf{Z}_p$ because then $f^1_{cris,p}$ evaluated on any $g-$fold product of an elliptic curve over R would be divisible by p which is not the case; cf., for instance, [8], p. 139. To check the equality $c^1_p = c^2_p$ we proceed as follows. Evaluating on $g-$fold products of elliptic curves we may assume that $g = 1$. Pick any pair $(a,b) \in \mathbf{M}(R)$ such that $f^i_{jet}\langle a,b\rangle \in \mathbf{Z}_p^\times$; cf. Lemma 6.13. Hence we also have $f^1_{cris,p}\langle a,b\rangle \in R^\times$. By Theorem 6.1 and by assertions 2) and 3) in Theorem 6.6 we have that

$$\tau_{a,b} = \frac{f^2_{jet}\langle a,b\rangle}{f^1_{jet}\langle a,b\rangle}, \tag{6.7}$$

where $\tau_{a,b}$ is the trace of the $p-$power Frobenius on $E_{a,b}\otimes \mathbf{F}_p$. By Lemma 6.4

$$\tau_{a,b} = \frac{f^2_{cris}\langle a,b\rangle}{f^1_{cris}\langle a,b\rangle}. \tag{6.8}$$

Equations (6.7), (6.8), (6.6) imply that $c^1_p = c^2_p$ and we are done. □

Lemma 6.15. *Let $R \in \mathbf{Witt}_p$, let $(E,\theta,\omega) \in \mathbf{M}_g(R)$, and assume (E,θ) is complementable. Set $f^i_{jet} := f^i_{jet,p}(E,\theta,\omega) \in R$, $i = 1,2$, and assume det $f^1_{jet} \in R^\times$. Then $(\omega^t, \Phi\omega^t)$ is a basis for $H = H^1_{DR}(E/R)$ and the matrix of $\Phi : H \to H$ with respect to this basis is*

$$\left[\begin{array}{cc} 0 & I \\ M & N \end{array}\right], \tag{6.9}$$

where

$$M = \phi(f^1_{jet})\cdot((f^1_{jet})^t)^{-1}, \quad N = f^2_{jet}\cdot(f^1_{jet})^{-1}.$$

Proof. By Lemma 6.14 *det* $f^1_{cris,p}(E,\theta,\omega) \in R^\times$. Now we conclude by combining Lemmas 6.4 and 6.14. □

6.6.1. At this point note that Theorem 2.4 on elliptic curves follows by simply putting together Theorem 6.11, Lemma 6.15, and Lemma 6.13.

6.6.2. Let us prove Theorem 2.2.

Proof. Let $B/\mathbf{Z}$ be a smooth affine scheme and let X/B be any curve of genus g. We will show that, after replacing B by an etale open set of it, part 2) of the Conjecture holds for X/B. We will then show that part 1) of the Conjecture holds too if we choose B carefully.

For part 2) of the Conjecture we allow ourselves to freely replace B by (non-empty) etale open sets of it. We may consider $(E,\theta,\omega)\in \mathbf{M}_g(B)$, with (E,θ) the Jacobian of X/B. By Theorem 6.9 we may assume the family

$$(f^r_{jet,p}(E/B,\theta,\omega))\in \prod_{p\notin S} gl_g(\mathcal{O}(J^r(B^{\wedge p})))$$

is Fermat. Then Lemma 6.15 directly implies that part 2) of the Conjecture holds for E/B (hence for X/B), with $f=(f_p)$ constructed, in the obvious way, from $f^1_{jet,p}, f^2_{jet,p}$, and with $g=(g_p)$ constructed from $det\ f^1_{jet,p}$.

For part 1) of the Conjecture let us assume the classifying map $B\to \mathcal{M}_g$ to the moduli scheme of curves (over $\mathbf{Z}$) is etale. Assume in what follows $g\geq 3$ (the case $g\leq 2$ follows, for instance, from the proof of Theorem 2.3 below). We may assume B is an open cover of a Zariski open set of $\mathcal{M}_g$ whose completion at each closed point gives formal moduli. Let $U\subset B$ be any non-empty open set. To conclude the proof it is enough to find $R\in \mathbf{Witt}_p$ and $P\in U(R)_!$ such that

$$det\ f^1_{jet}(E,\theta,\omega)\in R^\times, \tag{6.10}$$

where (E,θ) is the Jacobian of the curve corresponding to P. By Artin approximation [4], p. 91, it is enough to find an $R\in \mathbf{Witt}_p$ with algebraically closed residue field and $P\in U(R)$ such that (6.10) holds. Fix an $R\in \mathbf{Witt}_p$ with algebraically closed residue field k. Since $\mathcal{M}_g\otimes k$ is irreducible and the ordinary locus in it is open and dense [20] it follows that, with exception of finitely many characteristics (which we can always discard by enlarging S), the ordinary locus in $U\otimes k$ is non-empty. Pick a $k-$point in $U\otimes k$, and let C_k/k be fiber of X/B at that point. By Lemma 6.8 and by smoothness of $U/\mathbf{Z}$ one can lift the $k-$point defining C_k/k to an $R-$point $P\in U(R)$ such that the corresponding curve C/R has a Jacobian with Serre-Tate parameters $q_{ij}\in 1+pR$ satisfying $\det((q_{ij}-1)/p)\in R^\times$. We conclude by Theorem 6.7. □

6.6.3. Let us prove Theorem 2.3.

Proof. Let $B/\mathbf{Z}$ be a smooth affine scheme and $(E,\theta,\omega)\in \mathbf{M}_g(B)$. As in the preceding proof we will show that, after replacing B by an etale open set of it, part 2) of the Conjecture holds for E/B. We will then show that part 1) of the conjecture holds too if B is chosen carefully.

To check part 2) of the Conjecture we allow ourselves to freely replace B by etale open sets of it. By Theorem 6.9 we may assume

$$(f^r_{jet,p}(E/B,\theta,\omega))\in \prod_{p\notin S} gl_g(\mathcal{O}(J^r(B^{\wedge p})))$$

is Fermat. By further shrinking B in the etale topology we may also assume that (E,θ) is complementable. Then we can conclude part 2) of the Conjecture for E/B by using Lemma 6.15.

To check part 1) of the Conjecture consider the moduli scheme $\mathcal{A}_{g,N}$ of principally polarized Abelian schemes of dimension g with simplectic level $N\geq 3$ structure; this

can be viewed as a smooth scheme over $Spec\ \mathbf{Z}[1/N]$ that has irreducible geometric fibers [12], p. 364, [22], p. 60. We will show that part 1) of the Conjecture holds for an etale open set of $\mathcal{A}_{g,N}$ and for the universal Abelian scheme over it. Note that $det\ f^1_{jet,p}$ induces a section σ over an appropriate line bundle over $J^1(\mathcal{A}_{g,N}{}^{\wedge p})$. (Cf. [2] for more details on this.) Hence, over the Zariski open sets V of a cover of $\mathcal{A}_{g,N}$, σ defines functions $\sigma_{V,R} : V(R) \to R$. Let $R \in \mathbf{Witt}_p$ be fixed, with algebraically closed residue field k. As in the previous proof, it is enough, by Artin approximation, to show that any open set $U \subset \mathcal{A}_{g,N}$ contains a point $P \in U(R)$ such that $det\ f^1_{jet}\langle P\rangle \in R^\times$. Assume there is a U for which this is false. Since we assumed $\sigma_{U,R} : U(R) \to R$ takes values in pR it follows easily (using, say, (2.7) and (2.12) in [6]) that the section σ restricted to $J^1(U^{\wedge p})$ must be p times another section over $J^1(U^{\wedge p})$. Since $\mathcal{A}_{g,N} \otimes k$ is irreducible and reduced it follows that the section σ, viewed as a section over the whole of $J^1(\mathcal{A}_{g,N}{}^{\wedge p})$, is p times another section over $J^1(\mathcal{A}_{g,N}{}^{\wedge p})$. In particular $det\ f^1_{jet}(E,\theta,\omega) \in pR$ for any $(E,\theta,\omega) \in \mathbf{M}_g(R)$. But this clearly contradicts Lemma 6.13. This concludes our proof. □

7. Differential modular forms from $p-$jets: Fixed p

7.1. The aim of this section is to prove Theorem 6.6 and, as a by-product, Theorem 6.7. So in this section p is a fixed prime. Let $M^* \in \mathbf{Prol}_p$, $B = Spec\ M^0$, and let $(E,\theta,\omega) \in \mathbf{M}_g(B)$. Our aim is to construct a matrix

$$f^r_{jet,p}(E,\theta,\omega,M^*) \in gl_g(M^r)$$

and show that the rule $f^r_p := f^r_{jet,p}$ satisfies the conclusions of Theorems 6.6 and 6.7.

Set $B = Spec\ M^0$, $B^r = Spf\ M^r$; so $B^0 = B^{\wedge p}$. Now if (B_i) is an affine covering of B and if we can perform our construction for each B_i, it will be clear from our construction that the resulting matrices will glue together to give a matrix "over B", as desired. We claim that, after replacing B with each of the open sets of a suitable open covering, we may assume there exists an affine open covering $\mathcal{U} = (U_i)$ of E such that, for each i, the following conditions hold:

1) There is an index i_0 such that the image $Z = e(B)$ of the zero section $e : B \to E$ is entirely contained in U_{i_0}.

2) For each i one can choose etale coordinates on U_i/B, in the sense of Section 4.3.

3) The subscheme of U_{i_0} defined by the vanishing of its etale coordinates coincides with Z.

Our claim is clearly true if we only want to satisfy conditions 1) and 2). Assume that, after changing B as explained above, we found a covering (U_i) satisfying conditions 1) and 2) and let z be etale coordinates on U_{i_0}, so that the map $z : U_{i_0} \to \mathbf{A}^g_B$ is etale. The composition $z \circ e$ is a $B-$point of $\mathbf{A}^g_B$ which we may, of course, assume to be the point $o : B \to \mathbf{A}^g_B$ of coordinates $(0,...,0)$. Then the morphism $z^{-1}(o(B)) \to o(B) \simeq B$ is etale and has a section, induced by e. It follows that Z is open and closed in $z^{-1}(o(B))$. We can cover U_{i_0} with affine open sets each of which does not meet both Z and $z^{-1}(o(B))\backslash Z$. Replacing B, again, by the open sets of a suitable affine cover of it we reach a situation where all 3 conditions above are satisfied.

In what follows we choose our etale coordinates z on U_{i_0} such that they satisfy $\omega \equiv dz \bmod (z)^2$.

Now the sequence z of etale coordinates on U_{i_0} is trivially seen to be a regular sequence in $\mathcal{O}(U_{i_0})$, hence the graded ring associated to the ideal (z) in $\mathcal{O}(U_{i_0})$ is isomorphic to a ring of polynomials over M^0. This immediately implies that the $(z)-$adic completion of $\mathcal{O}(U_{i_0})$ is naturally isomorphic to $M^0[[z]]$. Taking completions along the zero sections of $E \times_B E$ and E, and the morphism between them induced by the group law we get, by the above remarks, a formal group law in $\Phi(z_1, z_2) \in M^0[[z_1, z_2]]^g$, attached to E. This will play a role later.

7.2. By the discussion in Section 4.3, for each i, the projection $J^r(U_i{}^{\wedge p}, M^*) \to U_i{}^{\wedge p} \times_{B^0} B^r$ has a section s_i. Let $N_p = N_p^r$ be the kernel of $J^r(E^{\wedge p}, M^*) \to E^{\wedge p} \times_{B^0} B^r$. For any i, j we may consider the difference, in E, of the sections s_i, s_j; it induces morphisms

$$(*) \qquad s_i - s_j : U_{ij}{}^{\wedge p} \times_{B^0} B^r \to N_p,$$

where $U_{ij} := U_i \cap U_j$.

7.3. Let

$$l(z) = \sum_{n \geq 1} a_{\mathbf{n}} z^{\mathbf{n}}$$

be the logarithm of the formal group law Φ attached to E and let e be the exponential. On the other hand, note that by Section 4.3, N_p identifies, as a formal scheme, with the ($p-$adic completion of the) affine space $(\mathbf{A}^{rg}_{M^r})^{\wedge p}$ with coordinates $z' = \delta z, z'' = \delta^2 z, ..., z^{(r)} = \delta^r z$. Via this identification, the group law on N_p induces a group law on $(\mathbf{A}^{rg}_{M^r})^{\wedge p}$. This group law can be explicitly computed in terms of the formal group law Φ as follows. As for E/B, one can attach to $J^r(E^{\wedge p})$ a formal group law over the ring M^r; it will be given by the tuple of formal series $(\Phi, \delta\Phi, ..., \delta^r\Phi)$ in the variables $\mathbf{z} = (z_1, z_2)$, $\mathbf{z}' = (z_1', z_2')$,..., $\mathbf{z}^{(r)} = (z_1^{(r)}, z_2^{(r)})$. The formal group law of N_p is given, then, by the tuple

$$([\delta\Phi] \circ [0, \mathbf{z}', ..., \mathbf{z}^{(r)}], ..., [\delta^r\Phi] \circ [0, \mathbf{z}', ..., \mathbf{z}^{(r)}]).$$

As noted in Section 5.2, however, these are restricted power series (rather than mere formal power series), so the addition $[+]$ on $(\mathbf{A}^{rg}_{M^r})^{\wedge p}$ induced by that on N_p is given by precisely this tuple. Let us consider, following Section 5.2, the series

$$L_p^s = L_p^s(z', ..., z^{(s)}) := \frac{1}{p}[l^{\phi^s}] \circ [\phi^s(z)] \circ [0, z', ..., z^{(s)}] \in M^s[z', ..., z^{(s)}]^{\wedge p}$$

for $1 \leq s \leq r$. By Proposition 5.1 , $L_p^s \equiv (z')^{p^{s-1}} \mod (p)$, and so $L_p^s \equiv (L_p^1)^{p^{s-1}} \mod (p)$. Also, by Proposition 5.2, the following formula holds:

$$L_p^s((z_1', ..., z_1^{(s)})[+](z_2', ..., z_2^{(s)})) = L_p^s(z_1', ..., z_1^{(s)}) + L_p^s(z_2', ..., z_2^{(s)}).$$

The pull-back via the map $(*)$ in Section 7.2 of the coordinates $z', ..., z^{(r)}$ on $\mathbf{A}^{rg}$ gives rise to column vectors

$$\alpha_{ijp}^1, ..., \alpha_{ijp}^r \in \mathcal{O}(U_{ij}{}^{\wedge p} \times_{B^0} B^r)^g.$$

Define, for $1 \leq s \leq r$,

$$\varphi_{ijp}^s := L_p^s(\alpha_{ijp}^1, ..., \alpha_{ijp}^s) \in \mathcal{O}(U_{ij}{}^{\wedge p} \times_{B^0} B^r)^g.$$

These are cocycles that define (column vectors of) cohomology classes

$$\varphi_p^s \in H^1((E \otimes M_p^s)^{\wedge p}, \mathcal{O}_{(E \otimes M_p^s)^{\wedge p}})^g = H^1(E \otimes M_p^s, \mathcal{O}_{E \otimes M_p^s})^g.$$

Now the isomorphism $\theta_* : H^0(E, T_{E/B}) \to H^1(E, \mathcal{O})$ induced by θ at the level of Lie algebras induces an isomorphism still denoted by

$$\theta_* : H^0(E \otimes M_p^s, T_{E\otimes M_p^s/M_p^s}) \to H^1(E \otimes M_p^s, \mathcal{O}_{E\otimes M_p^s}).$$

We can define

$$f_p^s = f_p^s(E, \theta, \omega, M^*) := \langle \theta_*^{-1}\varphi_p^s, \omega^t\rangle \in gl_g(M_p^s),$$

where $\langle\ ,\ \rangle$ is the natural pairing between sections of the tangent sheaf T and sections of the cotangent sheaf Ω^1. If, in all these definitions we keep s fixed and we increase r, then, of course, f_p^s does not change. Note that, as it stands, the definition of f_p^s depends a priori on the choice of the etale coordinates z.

Lemma 7.1. *f_p^r depends on M^* and on the isomorphism class of (E, θ, ω) only (but not on the choice of z).*

Proof. We will show that φ_{ijp}^s depend on (E, θ, ω) only, but not on z. Start by noting that

$$\omega(z) = d(l(z)) = \frac{\partial l}{\partial z}(z)dz.$$

On the other hand, if $\tilde{z} = u(z) \in M^0[[z]]^g$, $u(0) = 0$,

$$det\left(\frac{\partial u}{\partial z}(0)\right) \in (M^0)^\times$$

and $\tilde{l}$ is the logarithm with respect to $\tilde{z}$, then we have

$$\tilde{l}(u(z)) = \frac{\partial u}{\partial z}(0) \cdot l(z).$$

If we assume, in addition, that $\omega \equiv d\tilde{z} \bmod (z)$, then it follows that $\frac{\partial u}{\partial z}(0)$ is the identity matrix hence $\tilde{l}(u(z)) = l(z)$, in other words $[\tilde{l}] \circ [u(z)] = [l]$. It follows that $[\tilde{l}^{\phi^s}] \circ [u^{\phi^s}(z)] = [l^{\phi^s}]$. Let $\tilde{L}_p^s$, $\tilde{\alpha}_{ijp}^s$, and $\tilde{\varphi}_{ijp}^s$ be the corresponding quantities constructed starting with the parameters $\tilde{z}$. We have

$$\begin{aligned}
\tilde{\varphi}_{ijp}^s &:= \tilde{L}_p^s(\tilde{\alpha}_{ijp}^1, ..., \tilde{\alpha}_{ijp}^s) \\
&= \frac{1}{p}[\tilde{l}^{\phi^s}] \circ [\phi^s(z)] \circ [0, \tilde{\alpha}_{ijp}^1, ..., \tilde{\alpha}_{ijp}^s] \\
&= \frac{1}{p}[\tilde{l}^{\phi^s}] \circ [\phi^s(z)] \circ [u, \delta u, ..., \delta^s u] \circ [0, z', ..., z^{(s)}] \circ [\alpha_{ijp}^1, ..., \alpha_{ijp}^s] \\
&= \frac{1}{p}[\tilde{l}^{\phi^s}] \circ [\phi^s(u(z))] \circ [0, z', ..., z^{(s)}] \circ [\alpha_{ijp}^1, ..., \alpha_{ijp}^s] \\
&= \frac{1}{p}[\tilde{l}^{\phi^s}] \circ [u^{\phi^s}(z)] \circ [\phi^s(z)] \circ [0, z', ..., z^{(s)}] \circ [\alpha_{ijp}^1, ..., \alpha_{ijp}^s] \\
&= \frac{1}{p}[l^{\phi^s}] \circ [\phi^s(z)] \circ [0, z', ..., z^{(s)}] \circ [\alpha_{ijp}^1, ..., \alpha_{ijp}^s] \\
&= L_p^s(\alpha_{ijp}^1, ..., \alpha_{ijp}^s) = \varphi_{ijp}^s
\end{aligned}$$

and our lemma follows. □

7.4. A computation similar to the one above shows that if $\tilde{\omega} = \lambda\omega$, where $\lambda \in GL_g(M^0)$, and if $\tilde{f}_p^s$ is the matrix attached to $(E, \theta, \tilde{\omega})$, then we have

$$\tilde{\varphi}_{ijp}^s = \lambda^{\phi^s} \cdot \varphi_{ijp}^s.$$

Then we have the following computation, showing that f_p^s defines a Siegel $\delta-$modular form:

$$f_p^s(E, \theta, \lambda\omega, M^*) = \langle \theta_*^{-1} \lambda^{\phi^s} \varphi_p^s, (\lambda\omega)^t \rangle$$
$$= \lambda^{\phi^s} \langle \theta_*^{-1} \varphi_p^s, \omega^t \rangle \lambda^t = \lambda^{\phi^s} \cdot f_p^s(E, \theta, \omega, M^*) \cdot \lambda^t.$$

7.5. The following computation shows that f_p^s is isogeny covariant. Let $(E_1, \theta_1, \omega_1)$, $(E_2, \theta_2, \omega_2) \in \mathbf{M}_g(S)$, and let $u : A_1 \to A_2$ be an isogeny of degree prime to p such that $u^*\omega_2 = \omega_1$. Note that the isomorphism

$$\gamma = u \circ u^t : E_2 \overset{\theta_2}{\to} \check{E}_2 \overset{\check{u}}{\to} \check{E}_1 \overset{\theta_1^{-1}}{\to} E_1 \overset{u}{\to} E_2$$

induces an isomorphism at the level of Lie algebras

$$\gamma_* : H^0(E_2, T_{E_2/B}) \overset{\theta_{2*}}{\to} H^1(E_2, \mathcal{O}) \overset{\check{u}_* = u^*}{\to} H^1(E_1, \mathcal{O})$$
$$\overset{\theta_{1*}^{-1}}{\to} H^0(E_1, T_{E_1/B}) \overset{u_*}{\to} H^0(E, T_{E_2/B}).$$

Then γ_* above is dual to $\gamma^* : H^0(E_2, \Omega) \to H^0(E_2, \Omega)$. Note that $\gamma^*\omega_2 = [u^t]\omega_2$. Also let $u^* : H^0(E_2, \Omega^1) \to H^0(E_1, \Omega^1)$ be the pull back induced by u; it is dual to the Lie algebra map u_* above. If φ_{ip}^s corresponds to $(E_i, \theta_i, \omega_i)$, then our construction implies that $\varphi_{1p}^s = u^*\varphi_{2p}^s = \check{u}_*\varphi_{2p}^s$. Hence we have

$$f_p^s(E_1, \theta_1, \omega_1, M^*) = \langle (\theta_{1*})^{-1} \varphi_{1p}^s, \omega_1^t \rangle$$
$$= \langle (\theta_{1*})^{-1} \check{u}_* \varphi_{2p}^s, u^*\omega_2^t \rangle$$
$$= \langle u_*(\theta_{1*})^{-1} \check{u}_* \varphi_{2p}^s, \omega_2^t \rangle$$
$$= \langle \gamma_*(\theta_{2*})^{-1} \varphi_{2p}^s, \omega_2^t \rangle$$
$$= \langle (\theta_{2*})^{-1} \varphi_{2p}^s, \gamma^*\omega_2^t \rangle$$
$$= \langle (\theta_{2*})^{-1} \varphi_{2p}^s, \omega_2^t \rangle \cdot [u^t]^t$$
$$= f_p^s(E_2, \theta_2, \omega_2, M^*) \cdot [u^t]^t.$$

This concludes the proof of isogeny covariance.

7.6. Let us check assertion 4 in Theorem 6.6 so let $v, \bar{H}$ be as in the discussion before Theorem 6.6. It follows from Proposition 5.1 that $\bar{\varphi}_p^r \equiv (\bar{\varphi}_p^1)^{p^{r-1}} \mod p$, where the upper bar denotes, as usual, the reduction mod p. Write $\varphi_p^1 = \mu \cdot \theta_* v$ for some $\mu \in gl_g(M)$. We have

$$\bar{f}_p^1 = \langle \bar{\theta}_*^{-1} \bar{\varphi}_p^1, \bar{\omega}^t \rangle = \langle \bar{\theta}_*^{-1} \bar{\mu} \bar{\theta}_* \bar{v}, \bar{\omega}^t \rangle = \bar{\mu} \langle \bar{v}, \bar{\omega^t} \rangle = \bar{\mu}.$$

Since $F^*(\bar{\theta}_* \bar{v}) = \bar{H} \cdot \bar{\theta}_* \bar{v}$ it follows that

$$(F^*)^k(\bar{\mu} \bar{\theta}_* \bar{v}) = \bar{\mu}^{F^k} \cdot \bar{H}^{F^{k-1}} \cdots \bar{H}^F \cdot \bar{H} \cdot \bar{\theta}_* \bar{v}.$$

We then have

$$\begin{aligned}\bar{f}_p^r &= \langle \bar{\theta}_*^{-1}\bar{\varphi}_p^r, \bar{\omega}^t\rangle \\ &= \langle \bar{\theta}_*^{-1}(F^*)^{r-1}\bar{\varphi}_p^1, \bar{\omega}^t\rangle \\ &= \langle \bar{\theta}_*^{-1}(F^*)^{r-1}(\bar{\mu}\bar{\theta}_*\bar{v}), \bar{\omega}^t\rangle \\ &= \langle \bar{\theta}_*^{-1}(\bar{\mu}^{F^{r-1}}\cdot \bar{H}^{F^{r-2}}\cdots \bar{H}^F\cdot \bar{H}\cdot \bar{\theta}_*\bar{v}), \bar{\omega}^t\rangle \\ &= \bar{\mu}^{F^{r-1}}\cdot \bar{H}^{F^{r-2}}\cdots \bar{H}^F\cdot \bar{H}\langle \bar{v}, \bar{\omega}^t\rangle \\ &= (\bar{f}_p^1)^{F^{r-1}}\cdot \bar{H}^{F^{r-2}}\cdots \bar{H}^F\cdot \bar{H}.\end{aligned}$$

7.7. Let us check assertion 2 in Theorem 6.6. Note that $f_p^1(E,\theta,\omega) = 0$ if and only if $J^1(E^{\wedge p}) \to E^{\wedge p}$ has a section hence if and only if the $p-$power Frobenius on $E\otimes(R/pR)$ lifts to an endomorphism of $E^{\wedge p}$. By Grothendieck's existence theorem the latter, if it exists, comes from an endomorphism of E and we are done.

7.8. Assertion 1 in Theorem 6.6 is easy and will be left to the reader. To conclude the proof of Theorem 6.6 we need to verify assertion 3. Let us assume $r \geq 2$ and $M^* = R^*$. For any square matrix f let f^* denote the adjoint of f; if f is a 1×1 matrix, then we set, by convention, $f^* = 1$. Consider the $1-$cocycle

$$c_{ijp}^r := (det\ f_p^1)\varphi_{ijp}^r - f_p^r(f_p^1)^*\varphi_{ijp}^1 \in \mathcal{O}(U_{ij}{}^{\wedge p})^g.$$

Note that its cohomology class c_p^r is trivial because

$$\langle \theta_*^{-1}c_p^r, \omega^t\rangle = (det\ f_p^1)f_p^r - f_p^r(f_p^1)^* f_p^1 = 0.$$

Consequently, as in Section 3.7, one can write $c_{ijp}^r = \gamma_{ip}^r - \gamma_{jp}^r$ for some $\gamma_{ip}^r \in (\mathcal{O}(U_i)^{\wedge p})^g$. Define

$$\Psi_i := (det\ f_p^1)L_p^r - f_p^r(f_p^1)^* L_p^1 + \gamma_{ip}^r \in ((\mathcal{O}(U_i)[z', ..., z^{(r)}])^{\wedge p})^g.$$

Consider the isomorphism

$$u_{ip} : J^r(U_i{}^{\wedge p}) \to U_i{}^{\wedge p}\times N_p \simeq U_i{}^{\wedge p}\times (\mathbf{A}^{rg})^{\wedge p} \tag{7.1}$$

that, at the level of points of formal schemes, sends each point x of $J^r(U_i{}^{\wedge p})$ into the pair $(\pi(x), x - s_i(\pi(x)))$, where $\pi : J^r(U_i{}^{\wedge p}) \to U_i{}^{\wedge p}$ is the natural projection. If we assume that $s_{i_0}(0) = 0$, then u_{i_0p} restricted to N_p is the identity. Via the above isomorphisms Ψ_{ip}^r give rise to elements

$$\psi_{ip}^r \in \mathcal{O}(J^r(U_i{}^{\wedge p})).$$

We claim that ψ_{ip}^r glue together to give an element

$$\psi_p^r \in \mathcal{O}(J^r(E^{\wedge p})).$$

Now $J^r(E^{\wedge p})$ can be viewed as obtained by gluing $U_i{}^{\wedge p}\times (\mathbf{A}^{rg})^{\wedge p}$ via the isomorphisms

$$\begin{aligned}&U^{\wedge p}\times (\mathbf{A}^{rg})^{\wedge p} \to U^{\wedge p}\times (\mathbf{A}^{rg})^{\wedge p}, \\ &(u', ..., u^{(r)}) \mapsto (u', ..., u^{(r)})[+](\alpha_{ijp}^1, ..., \alpha_{ijp}^r).\end{aligned}$$

The homomorphism property of L_p^r with respect to $[+]$ in Section 7.3 easily implies

$$\Psi_{ip}^r((z', ..., z^{(r)})[+](\alpha_{ijp}^1, ..., \alpha_{ijp}^r)) = \Psi_{jp}^r(z', ..., z^{(r)})$$

which proves our claim about the possibility of gluing ψ^r_{ip}. Note that if one replaces γ^r_{ip} by $\gamma^r_{ip} + \lambda_p$ for some $\lambda_p \in R$ such that $\psi^r_p(0) = 0$, then

$$\psi^r_p : J^r(E^{\wedge p}) \to \mathbf{G}_a{}^{\wedge p}$$

is a homomorphism; this is proved by noting that Ψ^r_{ip} vanishes at the origin of $J^r(E^{\wedge p})$, its restriction to N_p is a homomorphism and is "equivariant" with respect to the action of N_p, with N_p acting on the additive group by translations via the restriction of Ψ^r_{ip} to N_p. Next consider the group homomorphism

$$e(pz) : \mathbf{G}_a{}^{\wedge p} \to E^{\wedge p}$$

defined, at the level of rings by $z \mapsto e(pz)$. It induces a homomorphism

$$e(pz) : J^r(\mathbf{G}_a{}^{\wedge p}) \to J^r(E^{\wedge p}).$$

The composition $\psi^r_p \circ e(pz) : J^r(\mathbf{G}_a{}^{\wedge p}) \to \mathbf{G}_a{}^{\wedge p}$ sends $z \mapsto \sum a_i \phi^i(z)$, $a_i \in R$, and the latter, for $r = 2$, is the Picard-Fuchs operator of the tuple ψ^2_p. We now address the question of computing these coefficients a_i explicitly. Since $u_{i_0 p}$ is the identity modulo z, $\psi^r_p \circ e(pz)$ is congruent modulo z with

$$\frac{1}{p}\{(det\ f^1_p)[l^{\phi^r}] \circ [\phi^r(z)] \circ [0, z', ..., z^{(r)}] \circ [\delta(e(pz)), ..., \delta^r(e(pz))] \\ -f^2_p (f^1_p)^* [l^{\phi}] \circ [\phi(z)] \circ [0, z'] \circ [\delta(e(pz))]\} + u^r_p(z) \tag{7.2}$$

for some $u^r_p(z) \in (R[z]^{\wedge p})^g$. We want to set $z = 0$ in (7.2). Note that, if $s \leq r$,

$$[l^{\phi^s}] \circ [\phi^s(z)] \circ [0, z', ..., z^{(s)}] \circ [\delta(e(pz)), ..., \delta^s(e(pz))] \circ [0, z', ..., z^{(s)}] \\ = [l^{\phi^s}] \circ [\phi^s(z)] \circ [e(pz), \delta(e(pz)), ..., \delta^s(e(pz))] \circ [0, z', ..., z^{(s)}] \\ = [l^{\phi^s}] \circ [e^{\phi^s}] \circ [p\phi^s(z)] \circ [0, z', ..., z^{(s)}] \\ = p[\phi^s(z)] \circ [0, z', ..., z^{(s)}].$$

So we get that $\sum_i a_i \phi^i(z)$ is congruent modulo z to

$$(det\ f^1_p)[\phi^r(z)] - f^r_p (f^1_p)^* [\phi(z)].$$

We conclude that

$$\sum_i a_i \phi^i(z) = (det\ f^1_p)\phi^r(z) - f^r_p (f^1_p)^* \phi(z) + h^r_p z$$

with $h^r_p \in Mat(g \times g, R)$. This implies, in particular, assertion 4 in Theorem 6.6.

7.9. Let us prove Theorem 6.7. Set $k = R/pR$, $\bar{E} := E \otimes_R k$, $\bar{J}^1(E^{\wedge p}) := J^1(E^{\wedge p}) \otimes_R k$. By [5], Lemmas 4.2 and 4.4, our hypothesis on the Serre-Tate parameters implies that the class of the extension

$$0 \to \mathbf{G}^g_{a,k} \to \bar{J}^1(E^{\wedge p}) \to \bar{E} \to 0$$

in $Ext^1(\bar{E}, \mathbf{G}_{a,k}) \simeq Hom_k(H^0(\bar{E}, F^* \Omega^1_{\bar{E}/k}), H^1(\bar{E}, \mathcal{O}))$ is invertible as a linear map. By our proof of Theorem 6.6, this implies that $\det(f^1_p(E, \theta, \omega)) \in R^\times$ for any θ, ω. The ordinarity assumption translates into the fact that the Hasse-Witt matrix $\bar{H}(\bar{E}, \bar{\theta}, \bar{\omega})$ is non-singular. We conclude by assertions 3 and 4 in Theorem 6.6.

8. Differential modular forms from $p-$jets: p variable

The aim of this section is to prove Theorems 6.9, 6.11, and 6.12.

8.1. For the proof of Theorem 6.11 we shall assume we are in the following:

Situation 1. We assume E is an elliptic curve in Weierstrass form over B where

$$B := Spec\ M, \quad M = \mathbf{Z}_S[a_4, a_6, \Delta^{-1}],$$

a_4, a_6 being two variables and $\Delta = 4a_4^3 + 27a_6^2$. More precisely, as we will need to set up our notations, we let

$$U_1 = Spec\ M[x,y]/(f), \quad f = y^2 - x^3 - a_4x - a_6,$$
$$U_2 = Spec\ M[z,w]/(g), \quad g = w - z^3 - a_4zw^2 - a_6w^3$$

be glued via $z \mapsto x/y, w \mapsto 1/y$ to give an elliptic curve E/M with origin given by the subscheme Z of U_2 defined by the ideal (z,w). We let $\mathcal{U}$ be the covering of E consisting of U_1 and U_2 and we let $\omega_1 = \omega := dx/y$. We set $U = U_1 \cap U_2$. Note that $U = Spec\ M[x,y,y^{-1}]/(f)$. Also, for $r \geq 1$, if we take

$$M_r = \mathbf{Z}_S[a_4, a_6, a_4', a_6', a_4'', a_6'', ..., a_4^{(r)}, a_6^{(r)}, \Delta^{-1}],$$

where $a_4', a_6', a_4'', a_6'', ..., a_4^{(r)}, a_6^{(r)}$ are new variables, then $M_p^r := \mathcal{O}(J^r(B^{\wedge p}))$ equals ${M_r}^{\wedge p}$.

In order to prove Theorem 6.9 it is sufficient, as we noted in the remarks made following its statement, to prove the weaker version in which the words "Zariski open set" are replaced by "etale open set" and the words "Fermat" are replaced by "formally Fermat". Let us also note that one can make a series of reductions as follows. Our first remark is that if $(E,\theta,\omega), (E',\theta',\omega') \in \mathbf{M}_g(B)$, with B irreducible, and if E and E' become isogenous over the geometric generic point of B, then Theorem 6.9 is true for (E,θ,ω) if and only if it is true for (E',θ',ω'). Indeed after replacing B by an etale affine open set of it we may assume there is an isogeny between E and E' over B, whose degree is invertible on B; then we use the "covariance property" with respect to the $1-$forms and the isogeny covariance of f_p^r. Our second remark is that for any Abelian variety A over an algebraically closed field of characteristic zero there is an Abelian variety $\tilde{A}$ such that $A \times \tilde{A}$ is isogenous to the Jacobian of a curve. Using this remark, the first remark and the compatibility of f_p^r with products, we see that, in order to prove Theorem 6.9, it is enough to do it in case E/B is the Jacobian of a curve C/B equipped with a $B-$point. Now, by further replacing B with an etale dense open set of it, and using Corollary 3.8 and Section 7.1, we may assume, in Theorem 6.9, that we are in the following:

Situation 2. $B = Spec\ M/\mathbf{Z}$ possesses special etale coordinates, hence, by Proposition 4.1, the family of rings $(M_p^r) := (\mathcal{O}(J^r(B^{\wedge p})))$ is isomorphic in $\mathcal{F}\mathbf{Alg}$ to $({M_r}^{\wedge p})$, where M_r is a polynomial ring over M in several variables. (Note, by the way, that all these conditions are also true in Situation 1 above.) Moreover we assume E/B is the Jacobian of a smooth projective curve C/B of genus $g \geq 1$, possessing a $B-$point O, and we let $\alpha : C \to E$ be the Abel-Jacobi map corresponding to O. We assume we have an affine open covering $\mathcal{U} = (U_i)$ of E such that for each i, U_i/B has special etale coordinates in the sense of Section 4.3 and for any two open sets U_i and U_j in $\mathcal{U}$ we have that $U_{ij} := U_i \cap U_j$ is principal in both U_i and U_j. We also

assume the induced covering $\mathcal{U} \cap C$ of C is prepared (in the sense of Section 3.6). We finally assume that one of the open sets in the covering, call it U_{i_0}, contains the image of the zero section of E/B and we assume that the scheme whose ideal is generated by the chosen special etale coordinates on U_{i_0} coincides with the zero section of E/B. We will consider *any* principal polarization θ on E/B (this can be, for instance, the canonical polarization defined by C) and we let ω be a basis for $H^0(E, \Omega^1_{E/B})$.

We will show in both Situations 1 and 2 that, after suitably enlarging S, the family of matrices

$$(f_p^r(E, \theta, \omega)) \in \prod_{p \notin S} gl_g(M_r{}^{\wedge p})$$

is formally Fermat (and, indeed, Fermat for $g = 1$). We will treat Situations 1 and 2 simultaneously. (For this reason, in Situation 1, we use the notation $C = E$.) What we are going to do will be to go back to our construction in Section 7 and show, step by step, that all the relevant objects there form Fermat families.

The diagonal map $U_{ij} \to U_{ij} \times_B U_{ij}$ induces a morphism in $\mathcal{F}\mathbf{Sch}$:

$$(U_{ij}{}^{\wedge p} \times_{B^{\wedge p}} J^r(B^{\wedge p}))_{coarse} \to ((U_{ij} \times_B U_{ij})^{\wedge p} \times_{B^{\wedge p}} J^r(B^{\wedge p}))_{coarse}.$$

By Propositions 4.4 and 4.5 we get a morphism

$$\Delta : (U_{ij}{}^{\wedge p} \times_{B^{\wedge p}} J^r(B^{\wedge p}))_{ind, U_{ij}} \to ((U_{ij} \times_B U_{ij})^{\wedge p} \times_{B^{\wedge p}} J^r(B^{\wedge p}))_{ind, U_{ij} \times_B U_{ij}}. \tag{8.1}$$

Due to Proposition 4.7 in Situation 1 and to Proposition 4.1 in Situation 2 there exist sections

$$s_i : (U_i{}^{\wedge p} \times_{B^{\wedge p}} J^r(B^{\wedge p}))_{coarse} \to (J^r(U_i{}^{\wedge p}))_{coarse}$$

in $\mathcal{F}\mathbf{Sch}$ of the natural projections. Since U_{ij} is principal in both U_i and U_j, Corollary 4.6 implies that s_i and s_j induce sections in $\mathcal{F}\mathbf{Sch}$

$$s_{ij}, s_{ji} : (U_{ij}{}^{\wedge p} \times_{B^{\wedge p}} J^r(B^{\wedge p}))_{coarse} \to (J^r(U_{ij}{}^{\wedge p}))_{coarse},$$

respectively. By Section 4.5 we have an induced morphism

$$s_{ij} \times s_{ji} : ((U_{ij} \times_B U_{ij})^{\wedge p} \times_{B^{\wedge p}} J^r(B^{\wedge p}))_{ind, U_{ij} \times_B U_{ij}} \to (J^r((U_{ij} \times_B U_{ij})^{\wedge p}))_{full} \tag{8.2}$$

in $\mathcal{F}\mathbf{Sch}$. The inclusion $U_{ij} \times_B U_{ij} \to E \times_B E$ induces a morphism in $\mathcal{F}\mathbf{Sch}$

$$(J^r((U_{ij} \times_B U_{ij})^{\wedge p}))_{full} \to (J^r((E \times_B E)^{\wedge p}))_{full}. \tag{8.3}$$

The difference map $E \times_B E \to E$ induces a morphism in $\mathcal{F}\mathbf{Sch}$

$$(J^r((E \times_B E)^{\wedge p}))_{full} \to (J^r(E^{\wedge p}))_{full}. \tag{8.4}$$

Composing (8.1) through (8.4) we get a morphism in $\mathcal{F}\mathbf{Sch}$

$$s_{ij} - s_{ji} : (U_{ij}{}^{\wedge p} \times_{B^{\wedge p}} J^r(B^{\wedge p}))_{ind, U_{ij}} \to (J^r(E^{\wedge p}))_{full}. \tag{8.5}$$

Now we choose an open set $W \subset E$ as follows. In Situation 1 we let $W \subset U_2$ be the affine open set where $(1 - a_6 w^2)\partial g / \partial w$ is invertible. Then W contains the zero section Z of the projection $E \to B$ and z is a special etale coordinate on W/B that defines Z as a subscheme. In Situation 2 we let $W = U_{i_0}$; then, again, by our assumptions in Situation 2, W contains the zero section Z of the projection $E \to B$ and W has special etale coordinates that define Z scheme theoretically. After a linear change we may assume these coordinates z are such that $\omega \equiv dz \bmod (z)$.

Set $Y_p = W^{\wedge p} \times_{B^{\wedge p}} J^r(B^{\wedge p})$. By Proposition 4.1 and Section 4.4 there is a canonical trivialisation in $\mathcal{F}\mathbf{Sch}$

$$(J^r(W^{\wedge p}))_{full} \simeq (Y_p \times (\mathbf{A}^{rg})^{\wedge p})_{ind,W} = ((W \times \mathbf{A}^{rg})^{\wedge p} \times_{B^{\wedge p}} J^r(B^{\wedge p}))_{ind,W} \tag{8.6}$$

over $(Y_p)_{full}$, attached to z. Let $\pi_p : J^r(E^{\wedge p}) \to E^{\wedge p}$ be the natural projections and let $N_p := \pi_p^{-1}(Z^{\wedge p})$. Then (N_p) is closed in $(J^r(E^{\wedge p}))_{full}$ so it has a deduced Fermat structure $(N_p)_{ded,E}$ in the sense of Section 3.3. On the other hand (N_p) is also closed in $(J^r(W^{\wedge p}))_{full}$ so it has a different deduced structure $(N_p)_{ded,W}$. It is a trivial exercise to check, however, that we have an isomorphism in $\mathcal{F}\mathbf{Sch}$

$$(N_p)_{ded,E} \simeq (N_p)_{ded,W}. \tag{8.7}$$

Clearly the morphism (8.5) has the property that for each p the image of

$$U_{ij}{}^{\wedge p} \times_{B^{\wedge p}} J^r(B^{\wedge p}) \to J^r(E^{\wedge p})$$

is contained in N_p. By Proposition 3.1 the morphism (8.5) factors through a morphism in $\mathcal{F}\mathbf{Sch}$

$$(U_{ij}{}^{\wedge p} \times_{B^{\wedge p}} J^r(B^{\wedge p}))_{ind,U_{ij}} \to (N_p)_{ded,E}. \tag{8.8}$$

Composing with (8.7) we get a morphism in $\mathcal{F}\mathbf{Sch}$

$$s_{ij} - s_{ji} : (U_{ij}{}^{\wedge p} \times_{B^{\wedge p}} J^r(B^{\wedge p}))_{ind,U_{ij}} \to (N_p)_{ded,W}. \tag{8.9}$$

Now (8.6) induces an isomorphism in $\mathcal{F}\mathbf{Sch}$

$$(N_p)_{ded,W} \simeq ((Z \times \mathbf{A}^{rg})^{\wedge p} \times_{B^{\wedge p}} J^r(B^{\wedge p}))_{ded}, \tag{8.10}$$

where

$$((Z \times \mathbf{A}^{rg})^{\wedge p} \times_{B^{\wedge p}} J^r(B^{\wedge p}))_{ded}$$

is viewed as a closed family in

$$((W \times \mathbf{A}^{rg})^{\wedge p} \times_{B^{\wedge p}} J^r(B^{\wedge p}))_{ind,W},$$

viewed with the deduced structure from the latter in the sense of Section 3.3. It is a straightforward verification that we have an isomorphism in $\mathcal{F}\mathbf{Sch}$

$$((Z \times \mathbf{A}^{rg})^{\wedge p} \times_{B^{\wedge p}} J^r(B^{\wedge p}))_{ded} \to ((\mathbf{A}^{rg})^{\wedge p} \times J^r(B^{\wedge p}))_{ind,B}, \tag{8.11}$$

where $((\mathbf{A}^{rg})^{\wedge p} \times J^r(B^{\wedge p}))_{ind,B}$ has the structure induced from B in the sense of Section 3.2. From (8.9), (8.10), (8.11) we get a morphism in $\mathcal{F}\mathbf{Sch}$

$$\gamma := \gamma_{ij} : (U_{ij}{}^{\wedge p} \times_{B^{\wedge p}} J^r(B^{\wedge p}))_{ind,U_{ij}} \to ((\mathbf{A}^{rg})^{\wedge p} \times J^r(B^{\wedge p}))_{ind,B} \tag{8.12}$$

Note that, by Section 4.4, the coordinates on $\mathbf{A}^{rg}$ correspond, via the morphism obtained by composing (8.10) with (8.11), to $z', z'', ..., z^{(r)}$.

As in Section 7, the isomorphisms (8.10) and (8.11) induce, for each p, an isomorphism $N_p \simeq (\mathbf{A}^{rg})^{\wedge p} \times J^r(B^{\wedge p})$ and, via these isomorphisms, the group law on N_p induces a group law on $(\mathbf{A}^{rg})^{\wedge p} \times J^r(B^{\wedge p})$ that we computed there. The pull-back via (8.12) of the coordinates $z', ..., z^{(r)}$ on $\mathbf{A}^{rg}$ gives rise to a families

$$(\alpha^1_{ijp}), ..., (\alpha^r_{ijp}) \in \prod_{p \notin S} \mathcal{O}(U_{ij}{}^{\wedge p} \times_{B^{\wedge p}} J^r(B^{\wedge p}))^g \tag{8.13}$$

with the property that there exists a covering of U_{ij} with affine open sets such that for each open set V of the covering the images of (the components of) $(\alpha^1_{ijp}), ..., (\alpha^r_{ijp})$ in $\prod_{p \notin S} \mathcal{O}(V^{\wedge p} \times_{B^{\wedge p}} J^r(B^{\wedge p}))$ are Fermat families. Now by the same arguments as in Proposition 4.5 it is easy to see that $(\mathcal{O}(V^{\wedge p} \times_{B^{\wedge p}} J^r(B^{\wedge p})))$, with its product Fermat structure isomorphic to $(\mathcal{O}(V^{\wedge p} \times \mathbf{A}^{kr})^{\wedge p})$, with its standard Fermat structure, where

k is the relative dimension of $B/\mathbf{Z}_S$. Hence, upon enlarging S, there exist, by Proposition 3.2, sequences $(\alpha_{ijp}^{s\nu})$, $(\alpha_{ijp\nu}^{s})$, of elements in $\prod_{p\notin S}\mathcal{O}(U_{ij}{}^{\wedge p}\times_{B^{\wedge p}}J^r(B^{\wedge p}))^g$, with $(\alpha_{ijp}^{s\nu})$ Fermat families, such that

$$\alpha_{ijp}^{s}-\alpha_{ijp}^{s\nu}=p^{\nu}\alpha_{ijp\nu}^{s} \tag{8.14}$$

for $p\notin S$. The definition

$$\varphi_{ijp}^{s}:=L_p^s(\alpha_{ijp}^1,...,\alpha_{ijp}^s)$$

in the last section can be supplemented by defining

$$\varphi_{ijp}^{s\nu}:=L_p^s(\alpha_{ijp}^{1\nu},...,\alpha_{p}^{s\nu})\in\mathcal{O}(U_{ij}{}^{\wedge p}\times_{B^{\wedge p}}J^r(B^{\wedge p}))^g. \tag{8.15}$$

By (8.14) we have

$$\varphi_{ijp}^{s}-\varphi_{ijp}^{s\nu}=p^{\nu}\varphi_{ijp\nu}^{s} \tag{8.16}$$

for $\varphi_{ijp\nu}^{s}\in\prod_{p\notin S}\mathcal{O}(U_{ij}{}^{\wedge p}\times_{B^{\wedge p}}J^r(B^{\wedge p}))^g$. Note that, for p and s fixed, (φ_{ijp}^{s}) is a cocycle, i.e. an element in $Z^1(\mathcal{U},\mathcal{O}^g_{E^{\wedge p}\times_{B^{\wedge p}}J^r(B^{\wedge p})})$ while (φ_{ijp}^{s}) is a priori not; however, for fixed i,j,s the family $(\varphi_{ijp}^{s\nu})$ is Fermat, hence the family (φ_{ijp}^{s}) is formally Fermat. Let us consider the formally Fermat family of cocycles

$$(\alpha^*\varphi_{ijp}^{s})\in\prod_{p\notin S}\mathcal{O}(C_{ij}{}^{\wedge p}\times_{B^{\wedge p}}J^r(B^{\wedge p}))^g$$

obtained by restricting φ_{ijp}^{s} to the completions of $C_{ij}:=C\cap U_{ij}$. As in Section 3.7, this family induces a family

$$(\alpha^*\varphi_{p}^{s})\in\prod_{p\notin S}H^1(C\otimes M_s{}^{\wedge p},\mathcal{O}_{C\otimes M_s{}^{\wedge p}})^g$$

of (vectors whose components are) cohomology classes.

Now we can pair this family of cohomology classes $\alpha^*\varphi_p^s$, via Serre duality $\langle\ ,\ \rangle_C$ on C, with the $1-$forms $\alpha^*\omega$, pull backs of ω via the Abel-Jacobi map. We claim that there exists an invertible matrix $\Sigma\in GL_g(M)$, independent of p, such that

$$f_p^r(E,\theta,\omega)=\langle\alpha^*\varphi_p^s,\alpha^*\omega^t\rangle_C\cdot\Sigma^t.$$

Since, by Corollary 3.9, the family

$$(\langle\alpha^*\varphi_p^s,\alpha^*\omega^t\rangle_C)\in\prod_{p\notin S}gl_g(M_s{}^{\wedge p})$$

is formally Fermat, it will follow that so is $(f_p^r(E,\theta,\omega))$ which will close the proof of Theorem 6.9. To check the claim above consider the isomorphisms

$$\theta_*:H^1(E,\mathcal{O})\to H^0(E,T)\simeq H^0(E,\Omega^1)^D,$$

$$u:H^1(E,\mathcal{O})\overset{\alpha^*}{\to}H^1(C,\mathcal{O})\overset{s}{\to}H^0(C,\Omega^1)^D\overset{\alpha^{*D}}{\to}H^0(E,\Omega^1)^D,$$

where s is the Serre duality and the upper D means "$M-$linear dual". Then $\theta_*^{-1}u^{-1}=\beta^D$ for some $M-$linear automorphism β of $H^0(E,\Omega^1)$. Consider the isomorphism

$$\sigma:H^0(E,\Omega^1)\overset{\beta}{\to}H^0(E,\Omega^1)\overset{\alpha^*}{\to}H^0(C,\Omega^1)$$

and write $\sigma\omega = \Sigma \cdot \alpha^*\omega$. Then we have

$$\begin{aligned} f_p^r(E,\theta,\omega) &= \langle \theta_*^{-1}\varphi_p^r, \omega^t\rangle \\ &= \langle \theta_*^{-1}u^{-1}u\varphi_p^r, \omega^t\rangle \\ &= \langle \beta^D\alpha^{*D}s\alpha^*\varphi_p^r, \omega^t\rangle \\ &= \langle \sigma^D s\alpha^*\varphi_p^r, \omega^t\rangle \\ &= \langle s\alpha^*\varphi_p^r, \sigma\omega^t\rangle \\ &= \langle \alpha^*\varphi_p^r, \alpha^*\omega^t\rangle_C \cdot \Sigma^t \end{aligned}$$

and our claim is proved. This closes the proof of Theorem 6.9.

8.2. From now on we will assume we are in Situation 1 and concentrate on the proof of Theorem 6.11. Note that Σ above is easily seen, in Situation 1, to be merely a unit in the ring $\mathbf{Z}[1/6]$. After a normalization, we may, and will, assume $\Sigma = 1$.

The cohomology group $H^1((E \otimes_M M_r)^{\wedge p}, \mathcal{O}) \simeq H^1(E \otimes_M M_r, \mathcal{O})^{\wedge p}$ is a free M_r-module of rank one with basis the cohomology class of the Cech cocycle $x^2y^{-1} \in \mathcal{O}(U \otimes_M M_r)^{\wedge p}$. Assume now that

$$g_p := (\sum_{i,j\in\mathbf{Z}} a_{ijp}y^iw^j) + (\sum_{i,j\in\mathbf{Z}} b_{ijp}y^iw^j)x + (\sum_{i,j\in\mathbf{Z}} c_{ijp}y^iw^j)x^2 \in M_r[x,y,w]^{\wedge p}.$$

Then $g_p(x,y,y^{-1}) \in \mathcal{O}(U \otimes_M M_r)^{\wedge p}$, viewed as a Cech cocycle (for the covering $E = U_1 \cup U_2$, with values in the structure sheaf $\mathcal{O}_E$), is cohomologous to $g_{res,p}x^2y^{-1}$ where

$$g_{p,res} := (\sum_{i-j=-1} c_{ijp}) \in M_r$$

is the coefficient of x^2y^{-1} in $g_p(x,y,y^{-1})$. Moreover the difference $g_p - g_{p,res}x^2y^{-1}$ can be explicitly represented as a coboundary $g_{p1} - g_{p2}$ with

$$g_{p1} := (\sum_{i\geq j} a_{ijp}y^{i-j}) + (\sum_{i\geq j} b_{ijp}y^{i-j})x + (\sum_{i\geq j} c_{ijp}y^{i-j})x^2 \in \mathcal{O}(U_1 \otimes_M M_r)^{\wedge p},$$

$$g_{p2} := (\sum_{j>i} a_{ijp}w^{j-i}) + (\sum_{j>i} b_{ijp}w^{j-i-1})z + (\sum_{j>i+1} c_{ijp}w^{j-i-2})z^2 \in \mathcal{O}(U_2 \otimes_M M_r)^{\wedge p}.$$

(Here we view g_{pi} both as polynomials and as elements of $\mathcal{O}((U_i \otimes_M M_r)^{\wedge p})$; there is no ambiguity because these polynomials have degree ≤ 2 in x.) Note that the operations $g_p \mapsto g_{p,res}$, $g \mapsto g_{p1}$, $g \mapsto g_{p2}$ are additive maps on the space of all quadratic polynomials in x with coefficients in $M_r[y,w]^{\wedge p}$ and they vanish on polynomials divisible by $yw - 1$. Note also that g_{p2} vanishes for $z = w = 0$. If

$$(g_p) \in \prod_{p\notin S} M_r[x,y,w]^{\wedge p}$$

is a Fermat family (with respect to the standard Fermat structure), then, by Remark 2.16, (g_{p1}) is a Fermat family; it is an easy exercise to show that (g_{p2}) and $(g_{p,res})$ are Fermat families as well. It is convenient to give a name to the equality

$$g_p(x,y,y^{-1}) = g_{p,res}x^2y^{-1} + g_{p1} - g_{p2}. \tag{8.17}$$

We shall call it the *standard* decomposition of $g_p(x, y, y^{-1})$. Note that if a regular function on $U_1{}^{\wedge p} \cap U_2{}^{\wedge p}$ is given by $g_p(x, y, y^{-1})$, $\eta_p \in H^1(E, \mathcal{O})$ is the cohomology class defined by this function, and $\omega = dx/y$, then

$$\langle \eta_p, \omega \rangle = g_{p,res}.$$

Write

$$U = Spec\ M[x, y, y^{-1}]/(f) = Spec\ M[x, y, w]/(f, yw - 1).$$

Since we are in Situation 1 we will systematically drop the index 12, e.g. we simply denote $\alpha^s_{12p}, \alpha^{s\nu}_{12p}, \varphi^{s\nu}_{12p}, \varphi^s_{12p\nu}$ by $\alpha^s_p, \alpha^{s\nu}_p, \varphi^{s\nu}_p, \varphi^s_{p\nu}$ and let these be images of some series $A^s_p, A^{s\nu}_p, F^{s\nu}_p, F^s_{p\nu} \in M_s[x, y, w]^{\wedge p}$, where $p \notin S$, and $(A^{s\nu}_p)$ are Fermat. Set

$$F^s_p := L^s_p(A^1_p, ..., A^s_p), \quad F^{s\nu}_p := L^s_p(A^{1\nu}_p, ..., A^{s\nu}_p). \tag{8.18}$$

(Note that F^s_p lifts φ^s_p.) Now (8.16) yields

$$F^s_p = F^{s\nu}_p + p^\nu F^s_{p\nu} + fG^{s\nu}_p + (yz - 1)H^{s\nu}_p \tag{8.19}$$

for some $G^{s\nu}_p, H^{s\nu}_p \in M_2[x, y, w]^{\wedge p}$. Apply, to (8.19), the (additive) operator

$$r_f : M_s[x, y, w]^{\wedge p} \to M_s[x, y, w]^{\wedge p}$$

that takes the remainder in the division by f, where f is viewed as a monic polynomial of degree 3 in x. This operator kills multiples of f and takes Fermat families into Fermat families, by Remark 2.14. Replacing the terms in (8.19) by their images under r_f we may assume that all terms in (8.19) are polynomials of degree ≤ 2 in x and $G^{s\nu}_p = 0$. Now apply the operators introduced before (8.17); we get

$$F^s_{p,res} = F^{s\nu}_{p,res} + p^\nu F^s_{p\nu,res}, \quad F^s_{pi} = F^{s\nu}_{pi} + p^\nu F^s_{p\nu i}, \quad i = 1, 2. \tag{8.20}$$

Then $f^s_p := f^s_p(E, \theta, dx/y) = F^s_{p,res}$; also $(f^{s\nu}_p) := (F^{s\nu}_{p,res})$ are Fermat families. Hence

$$(f^s_p) \in \prod_{p \notin S} M_s{}^{\wedge p}$$

are formally Fermat families. By further enlarging S we may assume, by Proposition 3.4, that (f^s_p) are Fermat families. This closes the proof of Theorem 6.11.

8.3. We conclude by proving Theorem 6.12.

Proof. We will borrow notations from the previous discussion. Recall that (F^r_{pi}), viewed as elements of

$$\prod_{p \notin S} \mathcal{O}(U_i \otimes_M M_r)^{\wedge p},$$

are formally Fermat. Also, by manipulations similar to the ones in the beginning of this section one easily shows that the family

$$(u_{ip}) : (J^r(U_i{}^{\wedge p}))_{full} \to (U_i{}^{\wedge p} \times (\mathbf{A}^{rg})^{\wedge p} \times_{B^{\wedge p}} J^r(B^{\wedge p}))_{ind, U_i} \tag{8.21}$$

considered already in the proof of Theorem 6.6 is Fermat. Composing (8.21) with the inverse of (8.6) we get a Fermat family of maps from the right-hand side of (8.6) to the right-hand side of (8.21); hence, specializing to the case $r = 1$ and due to Proposition 3.2, we may assume (after enlarging S) that the family induced by u_{2p}

$$\mathcal{O}(U_2 \otimes_M M_1)[z']^{\wedge p} \to \mathcal{O}(W \otimes_M M_1)[z']^{\wedge p} \tag{8.22}$$

takes z' into a formally Fermat family which is congruent to z' mod z hence has the form $(z' + zv_p)$ for some v_p. Of course (8.22) will take F^1_{p2} into the natural restriction of F^1_{p2}. Next write W in the form

$$W = Spec(M[z,w]/(g))_H = Spec\ \mathbf{Z}[a_4, a_6, z, w, t]/(g, tH - 1),$$

where $H = \Delta(1 - a_6 w^2)\frac{\partial g}{\partial w}$; note that $H(0,0) = \Delta$.

Claim. One can write

$$zv_p = zv_p^* + z^2 v_p^{**} + zwv_p^{***}$$

for some $v_p^*, v_p^{**}, v_p^{***}$ with (v_p^*) formally Fermat.

Indeed one can write v_p as the class of $V_p \in \mathbf{Z}_p[a_4, a_6, z, z', w, t]^{\wedge p}$ such that zV_p is in the ideal generated by $V_p^{(n)}$, p^n, g, $Ht - 1$, with $(V_p^{(n)})$ Fermat. Taking d/dz and setting $z = w = 0$ we get that $V_p|_{z=w=0}$ is formally Fermat and we are done by letting v_p^* be the image of the latter.

By Lemma 4.2 there is a Fermat family $(w_p(z)) \in \prod_{p \notin S} M[z]^{\wedge p}$ such that $g(pz, pw_p(z)) = 0$. Making the substitution $z \mapsto p^{-1}e(pz)$ we get

$$g(e(pz), pw_p(p^{-1}e(pz))) = 0. \tag{8.23}$$

We define a family of M_1-algebra maps

$$\mathcal{O}(W \otimes_M M_1)[z']^{\wedge p} \simeq \mathcal{O}(J^1(W^{\wedge p})) \to M_1[z, z']^{\wedge p} \tag{8.24}$$

by sending

$$z^{(i)} \mapsto \delta^i(e(pz)),$$
$$w^{(i)} \mapsto \delta^i(pw_p(p^{-1}e(pz))),$$
$$t^{(i)} \mapsto \delta^i[H(e(pz), pw_p(p^{-1}e(pz)))^{-1}].$$

The right-hand side of the above formulae is trivially seen to be Fermat, hence (8.24) is Fermat. Let

$$\Sigma_1 := L^1_p(z') - F^1_{p1} \in \mathcal{O}(U_1 \otimes_M M_1)[z']^{\wedge p},$$
$$\Sigma_2 := L^1_p(z') - F^1_{p2} \in \mathcal{O}(U_2 \otimes_M M_1)[z']^{\wedge p}.$$

By the claim above the composition of (8.22) and (8.24) sends Σ_2 into a family of the form

$$\frac{1}{p} l^\phi(p(\delta(e(pz)) + e(pz)m_p^* + e(pz)^2 m_p^{**} + e(pz)pw_p(p^{-1}e(pz))m_p^{***})) \\ -F^1_{p2}(e(pz), pw_p(p^{-1}e(pz))), \tag{8.25}$$

where (m_p^*) is the image of (v_p^*); so (m_p^*) is formally Fermat, hence Fermat. Hence the result m_p^0 obtained by setting $z = z', z = 0$ in m_p^* will also form a Fermat family in the product of the $M_1{}^{\wedge p}$'s. This immediately implies that the coefficient of z in (8.25) has the form pk_p, where $(k_p) \in \prod M_1{}^{\wedge p}$ is Fermat. On the other hand the coefficient of z' in (8.25) is immediately seen to be p (just set $z = 0$ in (8.25)).

Now, for any point $P = (a, b) \in M(R)$ such that $f^1\langle a, b\rangle = 0$, we have an induced map $M_1 \to R$; let σ_1, σ_2 be the images of Σ_1, Σ_2 in

$$\mathcal{O}(U_1 \otimes R)[z']^{\wedge p},\ \mathcal{O}(U_2 \otimes R)[z']^{\wedge p}.$$

Then, due to the condition $f^1\langle a,b\rangle = 0$, σ_1 and σ_2 glue together to give a homomorphism $J^1((E\otimes R)\hat{}^p) \to \mathbf{G}_a$, hence a $\delta-$character of order 1 of E whose Picard-Fuchs operator $\Lambda_{a,b} = \lambda_1\phi(z) + \lambda_0 z$, $\lambda_0, \lambda_0 \in R$, is obtained by specializing (8.25) to R. Since the coefficient of z' in $\Lambda_{a,b}$ is p, we conclude that $\lambda_1 = 1$. Moreover $\lambda_0 = pk\langle a,b\rangle$. We conclude that

$$\Lambda_{a,b} = \phi(z) - pk\langle a,b\rangle.$$

□

References

1. M. Barcau, *Isogeny covariant differential modular forms and the space of elliptic curves up to isogeny*, Compositio Math. 137 (2003), 237-273. MR1988499
2. M.Barcau, A.Buium, *Siegel differential modular forms*, International Math. Res. Notices 28 (2002), 1459-1503. MR1908022 (2003g:11044)
3. P. Berthelot, A. Ogus, *F-isocrystals and De Rham cohomology I*, Invent. Math. 72 (1983), 159-199. MR0700767 (85e:14025)
4. S. Bosch, W.Lutkebohmert, M. Raynaud, *Neron Models*, Springer Verlag, 1990. MR1045822 (91i:14034)
5. A. Buium, *Differential characters of Abelian varieties over p−adic fields*, Invent. Math. 122 (1995), 309-340. MR1358979 (96h:14036)
6. A. Buium, *Geometry of p−jets*, Duke J. Math. 82, 2 (1996), 349-367. MR1387233 (97c:14029)
7. A. Buium, *Differential characters and characteristic polynomial of Frobenius* , J. reine angew. Math. 485 (1997), 209-219. MR1442195 (98b:14023)
8. A. Buium, *Differential modular forms*, J. reine angew. Math. 520 (2000), 95-167. MR1748272 (2002d:11042)
9. A. Buium, *Infinitesimal Mordell-Lang*, J. Number Theory 90 (2001), 185-206. MR1858073 (2002j:11062)
10. B. Dwork, *A deformation theory for the zeta function of a hypersurface*, Proc. Intl. Cong. Math. (1962), 249-258. MR0175895 (31:171)
11. B. Dwork, A. Ogus, *Canonical liftings of Jacobians*, Composition Math. 58 (1986), 111-131. MR0834049 (87g:14021)
12. G. Faltings, Ch-L. Chai, *Degeneration of Abelian varieties*, Ergebnisse 3.22, Springer, Berlin, New York, 1990. MR1083353 (92d:14036)
13. P. Griffiths, J. Harris, *Principles of algebraic geometry*, Reprint of the 1978 original, Wiley Classics Library, John Wiley & Sons, Inc., New York, 1994. MR1288523 (95d:14001)
14. M. Hazewinkel, *Formal Groups and Applications*, Academic Press, 1978. MR0506881 (82a:14020)
15. C. Hurlburt, *Isogeny covariant differential modular forms modulo p*, Compositio Math. 128 (2001), 17-34. MR1847663 (2002i:11053)
16. Y. Ihara, *On Fermat quotient and "differentiation" of numbers*, RIMS Kokyuroku 810 (1992), 324-341, (in Japanese). English translation by S. Hahn, Univ. of Georgia preprint. MR1248209 (94m:11136)
17. S. Lang, *Algebraic number theory*, Springer, Berlin, New York, 1986. MR1282723 (95f:11085)
18. N. Katz, W. Messing, *Some consequences of the Riemann hypothesis for varieties over finite fields*, Invent. Math. 23 (1974), 73-77. MR0332791 (48:11117)
19. W. Messing, *The crystals associated to Barsotti-Tate groups: with applications to abelian schemes*, LNM 264, Springer, Berlin, New York, 1972. MR0347836 (50:337)
20. L. Miller, *Curves over finite fields with invertible Hasse-Witt matrices*, Math. Ann. 197 (1972). MR0314849 (47:3399)
21. P. Monski, G. Washnitzer, *The construction of formal cohomology sheaves*, Proc. Nat. Acad. Sci. USA 52 (1964), 1511-1514. MR0171787 (30:2014)
22. F. Oort, *A stratification of a moduli space of polarized abelian varieties*, in: Moduli of Curves and Abelian Varieties, C. Fber and E. Looijenga eds., Aspects of Mathematics 33, Vieweg, 1999. MR1722538 (2001m:14065)
23. J.P. Serre, *Algebraic Groups and Class Fields*, Springer, 1988. MR0918564 (88i:14041)

24. J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, Berlin, New York, 1986. MR0817210 (87g:11070)
25. J.H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer, Berlin, New York, 1994. MR1312368 (96b:11074)
26. F. Voloch, *On a question of Buium*, Canad. Math. Bulletin, 43, 2 (2000), 205-209. MR1754028 (2001g:11005)

Department of Mathematics and Statistics, University of New Mexico, Albuquerque, New Mexico 87131

E-mail address: buium@math.unm.edu