Indag. Mathem., N.S., 12 (1), 113–124 March 26, 2001

# Grothendieck's conjecture for the Risch equation $y' = ay + b$

by Marius van der Put

*Department of Mathematics, University of Groningen, P.O. Box 800, 9700 AV Groningen, The Netherlands,*
*e-mail: mvdput@math.rug.nl*

Communicated by Prof. T.A. Springer at the meeting of November 27, 2000

ABSTRACT

A simple formulation of the Grothendieck's conjecture, some information on $p$-curvatures, recent history and elementary proofs for the equations $y' = ay$ and $y' = b$ are given in the first two sections. For an inhomogeneous equation $y' = ay + b$ we propose an extension of the problem. One has to distinguish three cases. A proof, using Elkies' result on supersingular primes for elliptic curves, covers part of the first case. The second case has a negative answer. The final case is shown to be related with recent progress in sieve theory. Some examples of degree two can be handled in this way.

## 1. A FORMULATION OF THE CONJECTURE

One considers a scalar linear differential operator

$$L(y) := y^{(n)} + a_{n-1}y^{(n-1)} + \cdots + a_1 y^{(1)} + a_0 y,$$

with all $a_i \in \mathbf{Q}(z)$. For almost all prime numbers $p$, i.e., with the exception of finitely many, the rational functions $a_i$ can be reduced modulo $p$. The reductions of the $a_i$ will be denoted by $a_{i,p}$. They belong to the field $\mathbf{F}_p(z)$ of the rational functions over the field of $p$ elements $\mathbf{F}_p$. The reduction of $L$ modulo $p$ will be denoted by $L_p$. Then $L_p$ is a linear differential operator over the differential field $\mathbf{F}_p(z)$. *Grothendieck's conjecture* in its simplest (and most important) form asserts that the following two statements are equivalent.

(1) $L(y) = 0$ *has n linearly independent (over the algebraic closure of* $\mathbf{Q}$*) solutions* $y_1, \ldots, y_n$*, which are algebraic over* $\mathbf{Q}(z)$.

(2) *For almost all p, the equation* $L_p(y) = 0$ *has n linearly independent solutions over the field* $\mathbf{F}_p(z^p)$ *in the field* $\mathbf{F}_p(z)$.

**Some comments.** If one wishes to work over a differential field with algebraically closed field of constants, then one can view $L$ as a differential operator over the field $\overline{\mathbf{Q}}(z)$.

The constants of the differential field $\mathbf{F}_p(z)$ (with the usual differentiation $\frac{d}{dz}$) is the field $\mathbf{F}_p(z^p)$. One can view $\mathbf{F}_p(z)$ as a vector space over $\mathbf{F}_p(z^p)$ with basis $1, z, \ldots, z^{p-1}$. The differential operator $L_p : \mathbf{F}_p(z) \to \mathbf{F}_p(z)$ is a $\mathbf{F}_p(z^p)$ linear map. We will show that statement (2) means that the equation $L_p(y) = 0$ has the maximum set of solutions that one can expect.

We start by proving the easy implication of Grothendieck's conjecture.

**Lemma 1.1.** *Statement* (1) *implies statement* (2).

**Proof.** Let us consider first the case where $y_1, \ldots, y_n \in \mathbf{Q}(z)$. One can form the 'Wronskian' $w$ which is the determinant of the matrix

$$\begin{pmatrix} y_1 & y_2 & \cdot & y_n \\ y_1^{(1)} & y_2^{(1)} & \cdot & y_n^{(1)} \\ y_1^{(2)} & y_2^{(2)} & \cdot & y_n^{(2)} \\ \cdot & \cdot & \cdot & \cdot \\ y_1^{(n-1)} & y_2^{(n-1)} & \cdot & y_n^{(n-1)} \end{pmatrix}.$$

One knows that linearly independence over the algebraic closure of $\mathbf{Q}$ of the $y_1, \ldots, y_n$ is equivalent to $w \neq 0$.

One takes now a prime $p$ such that the reductions $y_{1,p}, \ldots y_{n,p}, w_p$ of $y_1, \ldots, y_n, w$ make sense and that $w_p \neq 0$. This excludes finitely many primes. Suppose now that the $y_{1,p}, \ldots, y_{n,p}$ satisfy a non trivial relation $b_1 y_{1,p} + \cdots + b_n y_{n,p} = 0$ with $b_1, \ldots, b_n \in \mathbf{F}_p(z^p)$. Since the $b_1, \ldots, b_n$ are constants, one finds relations $b_1 y_{1,p}^{(j)} + \cdots + b_n y_{n,p}^{(j)} = 0$ for all $j \geq 1$. This implies that $w_p = 0$ and contradicts our assumption on $p$.

*The general case:* A finite extension $K \supset \mathbf{Q}(z)$, has the form $\mathbf{Q}(z)[t] := \mathbf{Q}(z)[T]/(F)$, where $F = T^d + b_{d-1}T^{d-1} + \cdots + b_0$ is an irreducible polynomial and $t$ is the residue of $T$. The differentiation $'$ of $\mathbf{Q}(z)$ extends uniquely to $K$. Indeed, this extension is determined by the value of the derivative $t'$ of $t$. The equation $F(t) = 0$ implies that $t' = -(b'_{d-1}t^{d-1} + \cdots + b'_1 t + b'_0)/F'_T(t)$, where $F'_T$ denotes the derivative of $F$ with respect to $T$. We choose $K$ such that the independent solutions $y_1, \ldots, y_n$ lie in $K$. The Wronskian of $y_1, \ldots, y_n$ is again denoted by $w$. One considers now primes $p$ such that:

(i) $b_{d-1}, \ldots, b_0 \in R_p$.
(ii) the discriminant of $F$ (with respect to $T$) is invertible in $R_p$.
(iii) $y_1, \ldots, y_n \in R_p$.
(iv) $w$ is an invertible element of $R_p[t]$.

This excludes finitely many primes. The ring $R_p[t]$ is invariant under differ-

entiation. Indeed, the discriminant of $F$ is invertible and thus $F_T'(t)$ is invertible in $R_p[t]$. Hence $t' \in R_p[t]$. The ideal $(p) \in R_p[t]$ is invariant under differentiation. After dividing by the ideal $(p)$ one finds an extension $\mathbf{F}_p(z) \subset R_p[t]/(p)$ such that the derivation of $\mathbf{F}_p(z)$ extends to $R_p[t]/(p)$. The latter ring can also be written as $\mathbf{F}_p(z)[T]/(\bar{F})$, where $\bar{F}$ is the reduction modulo $p$ of $F$. The discriminant of $\bar{F}$ is, by assumption, invertible. Then $R_p[t]/(p)$ is a product $M_1 \times \cdots \times M_s$ of separable field extensions $M_i$ of $\mathbf{F}_p(z)$. The differentiation of $\mathbf{F}_p(z)$ extends in a unique way to this product $M_1 \times \cdots \times M_s$. This extension coincides therefore with the derivation that we had above. Let $M = M_1$ and let $v_1, \ldots, v_n, \bar{w}$ denote the images of $y_1, \ldots, y_n, w$ in $M$. Then $\bar{w}$ is the Wronskian of $v_1, \ldots, v_n$. We conclude, as above, that $v_1, \ldots, v_n$ are linearly independent over the field of constants of $M$. Using that $M$ is separable over $\mathbf{F}_p(z)$, one can show that the field of constants of $M$ is just $M^p$ and that $1, z, \ldots, z^{p-1}$ is also a basis of $M$ over $M^p$. In other words $M = M^p \otimes_{\mathbf{F}_p(z^p)} \mathbf{F}_p(z)$. The natural extension of $L_p$ as differential operator to $M$ coincides with the extension of $L_p$ as $\mathbf{F}_p(z^p)$-linear operator on the vector space $\mathbf{F}_p(z)$ to an $M^p$-linear operator on $M$. Therefore the kernel of $L_p$ on $\mathbf{F}_p(z)$ and the kernel of $L_p$ on $M$ have the same dimension. The latter is $n$ and thus the dimension of the kernel of $L_p$ on $\mathbf{F}_p(z)$ is also $n$. □

**Some history of the conjecture.** A. Grothendieck seems to have formulated this conjecture around 1969. The first positive answer were B. Dwork's results, (approximately 1970, see [K2]) for ordinary hypergeometric equations. In 1972, N. Katz [K1] proved the conjecture for Gauss-Manin differential equations (this includes the ordinary hypergeometric equations). The work of T. Honda [Ho] (1974) on the conjecture (this includes order one equations) was posthumously published in 1981. There is a very general reformulation by N. Katz [K3] (1982) of the conjecture which links the Lie algebra of the differential Galois group of a connexion with $p$-curvatures. D. Chudnovsky and G. Chudnovsky [CC] (1985) claim a proof for order one equations over a function field over a number field. In 1989, F. Beukers and G. Heckman [BH] gave a proof for generalized hypergeometric differential equations. Y. Haraoka proved the conjecture for Pochhammer equations in 1994. In Katz' book [K4] 'Rigid local systems' (1996) the conjecture is proved for certain rigid differential equations. This includes all former cases where the conjecture was known. In 1997, Y. André [A2] was able to prove the conjecture in still greater generality (equations associated with Gauss-Manin differential equations). In particular, he gave the first complete proof for the case of order one equations over function fields over an algebraic number field.

Let us mention, finally, the first case where the conjecture is 'wide open'. This is the case of a scalar equations over $\mathbf{Q}(z)$ of order two (!) with four regular singular points, rational exponents and having differential Galois group, say SL(2). One has to show here that statement (2) is not valid.

It is further interesting to know that N. Katz has shown (see [K3]) that our simple formulation of Grothendieck's conjecture implies the most general form of the conjecture.

**The $p$-curvature**

Statement (1) is well known to be equivalent to: the differential Galois group of the equation is finite. There is also a short formulation for statement (2), namely: for almost all $p$, the $p$-curvature is 0. The definition of the $p$-curvature is more easily given for a differential operator in matrix form. Consider the differential operator $\partial := \frac{d}{dz} - A$, where $A$ is a matrix of size $n \times n$ with coefficients, say in the field $\mathbf{F}_p(z)$. More generally one may take a field $k$ of characteristic $p$ such that $[k : k^p] = p$. Then $k = k^p(z)$ for some $z$ and the differentiation $'$ on $k$ is given by $z' = 1$.

The operator $\partial$, acting upon the $n$-dimensional $k$-vector space $k^n$, is $k^p$-linear. We note that the notation is confusing and we will write $V := k^n$. The $p^{\text{th}}$ power $\partial^p$ is certainly again $k^p$-linear. But it so happens that $\partial^p$ is $k$-linear. Indeed, one easily verifies the rule $\partial \cdot z = z \cdot \partial + 1$ (as operators). A small calculation shows that $\partial^p z = z\partial^p$. This implies that $\partial^p$ is $k$-linear. The operator $\partial^p$ is called the *$p$-curvature* of $\partial$.

**Lemma 1.2.** (P. Cartier)
*Let the field $k$ be as above. The matrix differential operator $\partial = \frac{d}{dz} - A$, with $A$ a matrix of size $n \times n$ and with coefficients in $k$, has an $n$-dimensional solution space over $k^p$ if and only if its $p$-curvature $\partial^p$ is zero.*

**Proof.** The operator $\partial : V := k^n \to V$ is linear with respect to the subfield $k^p$ of $k$. Suppose that there are $e_1, \ldots, e_n \in V$ in the kernel of $\partial$ and linearly independent over $k^p$. Using formulas like $\partial(z^a e_1) = az^{a-1}e_1$, one easily finds that the $e_1, \ldots, e_n$ are linearly independent over $k$ itself. Thus $\partial^p$ is zero on the $k$-basis $e_1, \ldots, e_n$ of $V$. Hence $\partial^p = 0$.

On the other hand, suppose that $\partial^p = 0$. Then the $k^p$-linear map $\partial$ on $V$ is nilpotent. In particular, there is a non zero element $e_1 \in V$ with $\partial e_1 = 0$. The vector space $ke_1 \subset V$ is invariant under $\partial$. Thus there is an induced action of $\partial$ on the $n-1$-dimensional vector space $W := V/ke_1$. By induction, $W$ has a $k$-basis $f_2, \ldots, f_n$ with $\partial f_i = 0$. Lifting back to $V$ we find vectors $F_2, \ldots, F_n$ such that $e_1, F_2, \ldots, F_n$ is a $k$-basis of $V$ and such that $\partial F_i \in ke_1$ for all $i \geq 2$. Consider for instance $\partial F_i = g_i e_1$. Then $0 = \partial^{p-1} g_i e_1 = g_i^{(p-1)} e_1$ and thus $g_i^{(p-1)} = 0$. It is easy to see that this implies that there exists a $G_i \in k$ with $G_i' = g_i$. Define $e_i = F_i - G_i e_1$ for $i \geq 2$. Then $e_1, \ldots, e_n$ is a $k$-basis of $V$ with $\partial e_i = 0$ for all $i$. Then the kernel of $\partial$ on $V$ is $k^p e_1 + \cdots + k^p e_n$. □

**Remarks 1.3.** *The $p$-curvature of a matrix differential operator $\frac{d}{dz} - A$, where $A$ is $n \times n$ matrix with coefficients (say) in $\mathbf{Q}(z)$, can be given by a simple algorithm. For $n = 1$ the $p$-curvature of $\frac{d}{dz} - a$ is $a^{(p-1)} + a^p$. Also for $n = 2$ there is a closed formula for the $p$-curvature. No closed formula seems to exist for $n > 2$.* (see [P1,P2]).

In the sequel we will study differential equations of the type $y' = ay + b$ with $a, b \in \mathbf{Q}(z)$ and their reductions modulo primes $p$. We note that this in-

homogeneous equation (for $b \neq 0$) can be seen as a special case of a homogeneous equation of order two, namely the equation $(b^{-1}(y' - ay))' = 0$.

## 2. THE EQUATIONS $y' = b$ AND $y' = ay$

In this section we will prove Grothendieck's conjecture for the two equations above.

**Proposition 2.1.** *Let $b \in \mathbf{Q}(z)$. The following properties of the equation $y' = b$ are equivalent.*

(1) *All the residues of $bdz$ are zero.*
(2) *There is a solution which is algebraic over $\mathbf{Q}(z)$.*
(3) *There is a solution in $\mathbf{Q}(z)$.*
(4) *For almost all primes $p$ there exists a solution in $\mathbf{F}_p(z)$.*

**Proof.** (1) $\Rightarrow$ (2) is trivial. Let a solution $f$ be given which is algebraic over $\mathbf{Q}(z)$. Then $\frac{1}{s}\sum_{i=1}^{s} f_i \in \mathbf{Q}(z)$, where $f_1, \ldots, f_s$ are the conjugates of $f$, is also a solution of the equation. This proves (2) $\Rightarrow$ (3). Further (3) $\Rightarrow$ (4) is obvious.

Suppose now that (4) holds. We replace $\mathbf{Q}$ be a finite extension $K$ such that all the poles of $bdz$ are in $K \cup \{\infty\}$. The prime numbers $p$ are replaced by the primes $\underline{p}$ of the ring of integers of $K$. Consider a prime $\underline{p}$, for which $y' = b$ has a solution modulo $\underline{p}$, which does not divide any denominator of $b$ and such that the poles of $b$ are distinct modulo $\underline{p}$. One observes that the reduction of the residue $\mathrm{res}_a(bdz)$ modulo $\underline{p}$ is equal to the residue at $a$ modulo $\underline{p}$ the reduction modulo $\underline{p}$ of $bdz$. Since there is a solution of $y' = b$ modulo $\underline{p}$ one concludes that $\mathrm{res}_a(bdz)$ is zero modulo this $\underline{p}$. This holds for almost all $\underline{p}$ and thus $\mathrm{res}_a(bdz) = 0$. Therefore (1) holds. □

The following is a variation on a proof given by T. Honda [Ho].

**Proposition 2.2.** (T. Honda)
*Let $a \in \mathbf{Q}(z)^*$. The following are equivalent.*

(1) *All the poles (including a possible pole at $\infty$) of $adz$ have order 1 and all residues are in $\mathbf{Q}$.*
(2) *The equation $y' = ay$ has a non zero solution which is algebraic over $\mathbf{Q}(z)$.*
(3) *For almost all prime numbers $p$, the equation $y' = ay$ has a non zero solution in $\mathbf{F}_p(z)$.*

**Proof.** (1) $\Rightarrow$ (2). Choose a positive integer $m$ such that all the residues of $madz$ are integers. It is easily seen that $madz$ is equal to $\frac{df}{f}$ for some non zero $f \in \overline{\mathbf{Q}}(z)$, where $\overline{\mathbf{Q}}$ denotes the algebraic closure of $\mathbf{Q}$. Now $f^{1/m}$ is an algebraic solution of $y' = ay$.
(2) $\Rightarrow$ (3). This is a special case of lemma 1.1.
(3) $\Rightarrow$ (1). In the proof we replace $\mathbf{Q}$ be a finite extension $K$ such that all the poles of $adz$ are in $K \cup \{\infty\}$. The prime numbers are replaced by prime ideals $\underline{p}$ of the ring of integers of $K$ and the fields $\mathbf{F}_p$ are replaced by finite extensions.

Consider a prime $\underline{p}$ such that $adz$ can be reduced modulo $\underline{p}$, such that the poles of $adz$ are distinct modulo $\underline{p}$ and such that $y' = ay$ has a non zero solution $f$ modulo $\underline{p}$. One writes $f$ as a product $\prod_i (z - \alpha_i)^{m_i}$ with all $\alpha_i$ algebraic over $\mathbf{F}_p$ and all $m_i \in \mathbf{Z}$. One observes that the reduction of $adz$ modulo $\underline{p}$ is $\frac{df}{f} = \sum_i (m_i/(z - \alpha_i))dz$, has poles of order at most 1 and all its residues are in $\mathbf{F}_p$ for the prime number $p$ lying under $\underline{p}$. This holds for almost all $\underline{p}$. The conclusion is that $adz$ has at most poles of order 1 and that any residue $r$ at a pole is an algebraic number in $K$ which reduces modulo almost every prime $\underline{p}$ to an element in a prime field $\mathbf{F}_p$. If $r \notin \mathbf{Q}$ then by Čebotarev's density theorem, there is an infinite set of primes $\underline{p}$ of $K$ such that $r$ modulo $\underline{p}$ does not lie in the corresponding prime field $\mathbf{F}_p$. Thus $r \in \mathbf{Q}$. □

**Example 2.3.** The equation $y' = (1/(z^2 + 1))y$ has only the trivial algebraic solution $y = 0$ since the residues are in $\mathbf{Q}(i) \setminus \mathbf{Q}$. The prime numbers $p$ such that the equation has a non zero solution in $\mathbf{F}_p(z)$ are obviously the $p \equiv 1$ modulo 4.

## 3. ALGORITHMS FOR $y' = ay + b$

### 3.1. Solutions in the field $\mathbf{Q}(z)$

We suppose that both $a$ and $b$ are non zero. The reasoning (2) ⇒ (3) of proposition 2.1 applies here as well and therefore we are only interested in a possible solution in $\mathbf{Q}(z)$. The Risch algorithm for determining possible solutions $y \in \mathbf{Q}(z)$ works as follows. For every pole $\alpha \in \overline{\mathbf{Q}}$ of either $a$ or $b$ one determines an a priori lower bound for the order of $y$ at $\alpha$. This produces an expression $y = T/N$ with $T, N \in \mathbf{Q}[z]$ with $N$ monic and known and $T$ unknown. A calculation at $\infty$ yields a bound $d$ on the degree of $T$. Put $T = t_0 + t_1 z + \cdots + t_d T^d$ with unknown coefficients $t_i$. The equation $(T/N)' = a(T/N) + b$ reduces now to a set of linear equations for the $t_i$. Linear algebra finishes the algorithm.

### 3.2. Solutions in the field $\mathbf{F}_p(z)$

We suppose that both $a$ and $b$ are non zero. One considers the operator $L : \mathbf{F}_p(z) \to \mathbf{F}_p(z)$, given by $L(y) = y' - ay$. This operator is linear over the field $\mathbf{F}_p(z^p)$. There are two cases to treat:

(1) The equation $y' = ay$ has only the trivial solution $0 \in \mathbf{F}_p(z)$.

(2) There is a solution $y_0 \in \mathbf{F}_p(z)$, $y_0 \neq 0$.

In the first case the kernel of $L$ is 0 and so $L$ is bijective. Thus for any $b$ there is a unique solution $y$ of $y' = ay + b$.

In the second case one uses 'variation of constants', i.e., one writes $y = Fy_0$ and finds the equation $F' = y_0^{-1}b$. We may suppose that $y_0$ has the form $\prod (z - \alpha)^{m_\alpha}$ with $0 < m_\alpha < p$ and write $b = T/N$. We may replace the equation $F' = y_0^{-1}b$ by the equation $(Fy_0^p N^p)' = y_0^{p-1} N^{p-1} T \in \overline{\mathbf{F}}_p[z]$. Thus there is a solution $y$ if and only if the polynomial $y_0^{p-1} N^{p-1} T$ does not contain the terms $z^{p-1}, z^{2p-1}, z^{3p-1}, \ldots$.

## 4. THREE CASES FOR $y' = ay + b$

We will suppose that both $a$ and $b$ are non zero. Suppose that there is a solution $y \in \mathbf{Q}(z)$. Then for almost all primes $p$, the equation and the solution $p$ reduce nicely modulo $p$ and so there is a solution in $\mathbf{F}_p(z)$ of the reduced equation. The question is now:

*Suppose that the equation has a solution modulo p for almost all p. Does it follow that there is a solution in* $\mathbf{Q}(z)$*?*

The answer depends heavily on the nature of the homogeneous equation $y' = ay$ and we will consider three separate cases. In the first case $y' = ay$ is supposed to have an algebraic solution. The equation $y' = ay + b$ can be written as a second order equation $(b^{-1}(y' - ay))' = 0$. The assumptions are equivalent to: for almost all primes $p$ there are two independent solutions in $\mathbf{F}_p(z)$. The Grothendieck conjecture predicts then two independent solutions, algebraic over $\mathbf{Q}(z)$. In this special case, this means a solution $y \in \mathbf{Q}(z)$ of $y' = ay + b$. The other two cases that we consider are *not* special cases of Grothendieck's conjecture.

## 5. CASE 1: EQUATION $y' = ay$ HAS AN ALGEBRAIC SOLUTION

Let $f \neq 0$ be a solution of $y' = ay$, which is algebraic over $\mathbf{Q}(z)$. We apply 'variation of constants', i.e., $y = fF$ and equation $F' = \frac{b}{f}$. In terms of differential forms: $dF = \omega := \frac{b}{f}dz$. This differential form is now defined over the finite field extension $\mathbf{Q}(z,f)$ of $\mathbf{Q}(z)$. We translate the equation in more geometric terms.

Let $C/\mathbf{Q}$ denote the (projective, connected, non singular) curve over $\mathbf{Q}$ which has $\mathbf{Q}(z,f)$ as function field. Let $g$ denote its genus . Then we are given a differential form $\omega$. We assume that, for almost all primes $p$, the reduction of $\omega$ modulo $p$ is exact, and *we want to show that* $\omega$ *itself is exact.*

The reasoning (4) $\Rightarrow$ (1) of proposition 2.1 also yields that every residue of $\omega$ on $C$ is 0. In other words, $\omega$ is a differential form of the second kind and it suffices to consider its image in the De Rham cohomology group $H^1_{DR}(C)$ of the curve $C$. In testing whether the above statement is correct, it suffices to consider nice representatives of the $\mathbf{Q}$-vector space $H^1_{DR}(C)$ of dimension $2g$. For $g = 0$, (i.e, the case of proposition 2.1) there is nothing to prove. Thus the first new situation is $g = 1$. This occurs, for instance, for the differential equation $y' = ((1/2)/(z^3 + az + b))y + B$ such that $z^3 + az + b$ has a non zero discriminant and with suitable $B \in \mathbf{Q}(z)$. The curve $C = E$ is the elliptic curve given by equation $y^2 = v := x^3 + ax + b$ with $a, b \in \mathbf{Q}$. (Note that we have changed $z$ into $x$). The representatives of $H^1_{DR}(E)$ are $\omega = (\alpha + \beta x)\frac{dx}{y}$ with $\alpha, \beta \in \mathbf{Q}$. What we want to show is:

**Theorem 5.1.** *Let E denote the elliptic curve over* $\mathbf{Q}$ *given by the affine equation* $y^2 = x^3 + ax + b$. *If* $\omega = (\alpha + \beta x)\frac{dx}{y}$ *is exact modulo p for almost all p, then* $\alpha = \beta = 0$.

We start with some calculations in characteristic $p$. The function field of the reduced curve is equal to $\mathbf{F}_p(x) + \mathbf{F}_p(x)y$ with $y^2 = v$. In trying to solve $dF = \omega$ (modulo $p$), we write $F = A + By$. Then $dF = A'dx + (vB' + v'B/2)\frac{dx}{y}$ and so we have to solve $vB' + v'B/2 = \alpha + \beta x$. Put $f = v^{(p-1)/2}$ and write $B = fG$. Then we obtain an equation $v^pG' = (\alpha + \beta x)v^{(p-1)/2}$. The right hand side is a polynomial of degree $(3(p-1))/2$. Thus we see that $\omega$ modulo $p$ is exact if and only if $(\alpha + \beta x)v^{(p-1)/2}$ does not contain the term $x^{p-1}$. We consider first two easy examples.

**Example 1.** $v = x^3 + 1$. The coefficient of $x^{p-1}$ is, for $p \equiv 1$ modulo 3, equal to a (non-zero) binomial coefficient times $\alpha$. For $p \equiv 2$ modulo 3, this coefficient is equal to a (non-zero) binomial coefficient times $\beta$. The conclusion is: If $\omega$ is exact modulo $p$ for almost all $p$, then $\alpha = \beta = 0$.

**Example 2.** $v = x^3 + x$. The coefficient of $x^{p-1}$ is, for $p \equiv 1$ modulo 4, equal to a (non-zero) binomial coefficient times $\alpha$. For $p \equiv 3$ modulo 4, this coefficient is equal to a (non-zero) binomial coefficient times $\beta$. The conclusion is again: If $\omega$ is exact modulo $p$ for almost all $p$, then $\alpha = \beta = 0$.

**Remark.** The two examples above concern rather special elliptic curves $E$. As we will see in the sequel, the main property that we have used is that for 'half' of the primes $p$ the reduction of $E$ modulo $p$ is supersingular. This property also holds for any elliptic curve having complex multiplication and these curves provide other easy examples.

*In the general case*

$$(\alpha + \beta x)(x^3 + ax + b)^{(p-1)/2} =$$

$$(\alpha + \beta x)(x^{3(p-1)/2} + \cdots + C_{p-1}x^{p-1} + C_{p-2}x^{p-2} + \cdots)$$

and the coefficient of $x^{p-1}$ is equal to $\beta C_{p-2} + \alpha C_{p-1}$. The problem is of course that we have no 'closed formula' for the $C_{p-1}$ and $C_{p-2}$ (depending on $a, b$ and $p$). The first helpful result is:

**Lemma 5.2.** *$C_{p-1}$ and $C_{p-2}$ cannot both be zero.*

**Proof.** We will prove that for $a, b \in \overline{\mathbf{F}}_p$, such that $x^3 + ax + b$ has three distinct roots, not both polynomials $(x^3 + ax + b)^{(p-1)/2}$ and $x(x^3 + ax + b)^{(p-1)/2}$ are derivatives. This condition does not change if $x$ is replaced by $cx + d$, where $c, d \in \overline{\mathbf{F}}_p$ and $c \neq 0$. Thus we may replace the polynomial $x^3 + ax + b$ by $x(x-1)(x-\lambda)$ (with $\lambda \in \overline{\mathbf{F}}_p$ and $\lambda \neq 0, 1$). We view now $\lambda$ as a variable. The coefficients $C_{p-1}$ and $C_{p-2}$ of $F := (x(x-1)(x-\lambda))^{(p-1)/2}$ are functions of $\lambda$. In fact they are polynomials in $\lambda$ of degree $(p-1)/2$. The maybe surprising observation is that $C_{p-1}$ and $C_{p-2}$ satisfy a simple linear differential equation, namely

$$\frac{d}{d\lambda}\begin{pmatrix} C_{p-1} \\ C_{p-2} \end{pmatrix} = \begin{pmatrix} \frac{-1}{2(\lambda-1)} & \frac{1}{2\lambda(\lambda-1)} \\ \frac{-1}{2(\lambda-1)} & \frac{1}{2(\lambda-1)} \end{pmatrix} \begin{pmatrix} C_{p-1} \\ C_{p-2} \end{pmatrix}.$$

Let us accept this differential equation for a moment and consider a $\lambda_0 \in \overline{\mathbf{F}}_p, \lambda_0 \neq 0, 1, \infty$. Suppose that $C_{p-1}(\lambda_0) = C_{p-2}(\lambda_0) = 0$. Then all the derivatives of $C_{p-1}$ and $C_{p-2}$ at $\lambda_0$ are 0. Thus $C_{p-1}$ and $C_{p-2}$ are $p^{\text{th}}$ powers. This contradicts that $C_{p-1}$ and $C_{p-2}$ are polynomials of degree $(p-1)/2$.

The above differential equation is derived from the family of elliptic curves $y^2 = x(x-1)(x-\lambda)$, say over the field $\mathbf{Q}(\lambda)$ (called the Legendre family). The first De Rham cohomology group $H^1_{DR}$ is defined as before. On this vector space of dimension two over the field $\mathbf{Q}(\lambda)$ one can differentiate with respect to the variable $\lambda$. The rules for the differentiation can be taken to be: $\frac{d}{d\lambda}$ is zero on $x$ and $dx$ and $\frac{d}{d\lambda}y$ is the usual differentiation of $y$ as function of $\lambda$. Then one finds $\frac{d}{d\lambda}(\frac{dx}{y}) = \frac{1}{2(x-\lambda)}\frac{dx}{y}$ and $\frac{d}{d\lambda}(x\frac{dx}{y}) = \frac{x}{2(x-\lambda)}\frac{dx}{y}$. Both expressions are differential forms of the second kind and they are equal, modulo exact differentials, to $\frac{-1}{2(\lambda-1)}\frac{dx}{y} + \frac{1}{2\lambda(\lambda-1)}\frac{xdx}{y}$ and $\frac{-1}{2(\lambda-1)}\frac{dx}{y} + \frac{1}{2(\lambda-1)}\frac{xdx}{y}$. The differential equation that we constructed in this way is called the Gauss-Manin differential equation of the Legendre family. It can be verified that this is in fact equivalent to the hypergeometric equation with parameters $1/2, 1/2, 1$.

The above calculation remains valid over the field $\overline{\mathbf{F}}_p(\lambda)$ for any odd prime $p$. Over the latter field we may multiply the basis $\frac{dx}{y}, \frac{xdx}{y}$ of $H^1_{DR}$ with the 'constant' $y^p$. The new basis is then $Fdx, xFdx$. We will omit the $dx$ in the notation and, since we work modulo derivatives (of polynomials), we may replace $F$ and $xF$ by $C_{p-1}x^{p-1}$ and $C_{p-2}x^{p-1}$. After omitting term $x^{p-1}$ one obtains the linear differential equation above for $C_{p-1}, C_{p-2}$. □

Now we recall some results about reductions of an elliptic curve $E$ modulo a prime $p$. We only consider reductions which are again elliptic curves (this excluded finitely many primes). The reduction $\bar{E}$ of $E$ modulo $p$ is called *ordinary* if the group $\{g \in \bar{E}(\overline{\mathbf{F}}_p) \mid g^p = 1\}$ is cyclic of order $p$. In the contrary case the reduction (which is regular) is called *supersingular*. An easy criterion is: $E$ modulo $p$ is supersingular if and only if $C_{p-1} = 0$. It can further be shown that there are infinitely many primes $p$ such that $E$ modulo $p$ has an ordinary reduction. A rather deep result is Elkies' theorem (see [E]): Any elliptic curve over $\mathbf{Q}$ has supersingular reduction for infinitely many primes $p$. (The analogous statement for elliptic curves over a number field is not known to be true).

We apply now all this to the coefficient $\beta C_{p-2} + \alpha C_{p-1}$. For infinitely many primes $p$ we have that $C_{p-1} = 0$ and so $C_{p-2} \neq 0$. Thus $\beta = 0$. For infinitely many primes $C_{p-1} \neq 0$. Therefore $\alpha = 0$. This ends the proof of theorem 5.1 and of Grothendieck's conjecture for a genus 1 curve over $\mathbf{Q}$.

Now we compare theorem 5.1 with the literature. It is the genus 1 case of a theorem of D. Chudnovski and G. Chudnovski [CC], which reads as follows.

**Theorem 5.3.** *Let $C/K$ be a curve over a number field $K$ and let $\omega$ be a differential form on $C$.*

(1) *Suppose that for almost all primes p of K the differential form $\omega$ is exact modulo p, then $\omega$ is exact.*

(2) *Suppose that the equation $\frac{dF}{F} = \omega$ has a solution modulo p for almost all p. Then the equation $\frac{dF}{F} = \omega$ has a solution F which is algebraic over the function field of C.*

The proof of this theorem was not well understood. Recently, Y. André (see [A2]) gave a complete proof of the theorem. His method is totally different from our proof of theorem 5.1.

## 6. CASE 2: THE EQUATION $y' = ay$ HAS AN IRREGULAR SINGULARITY

The assumption on $y' = ay$ can also be restated as *adz* has some pole of order $\geq 2$. This implies that for almost all $p$, the equation $y' = ay$ has only the zero solution in $\mathbf{F}_p(z)$. As a consequence, the inhomogeneous equation $y' = ay + b$ has, for almost all $p$, a (unique) solution in $\mathbf{F}_p(z)$. However, in general there is no solution $y \in \mathbf{Q}(z)$. We give an *example*:

The equation $y' = y + z^{-1}$. The point $\infty$ is an irregular singular point. There is no solution in $\mathbf{Q}(z)$ and there is a solution modulo $p$ for all $p$. The link between those solutions modulo $p$ and something in characteristic zero is explained by considering the formal solution $y = \sum_{n \geq 1} (-1)^n (n-1)! z^{-n}$ at $z = \infty$. The amazing observation is that $y$ reduces modulo any prime $p$ to a polynomial solution (in the variable $z^{-1}$) with coefficients in $F_p$. This example illustrates recent work of Y. André (see [A1]) on arithmetic properties of Gevrey series solutions of differential equations.

## 7. CASE 3: $y' = ay$ HAS ONLY REGULAR SINGULARITIES, BUT NO ALGEBRAIC SOLUTION $\neq 0$

For this situation, F. Beukers has proposed the following extension of Grothendieck's conjecture.

**Conjecture 7.1.** *Suppose that $y' = ay + b$ has for almost all primes p a solution modulo p, then there is a solution in $\mathbf{Q}(z)$.*

As a test, we consider one rather interesting equation, namely

$$y' = \frac{az + b}{z^2 + 1} y + \frac{1}{z^2 + 1}, \text{ with } a, b \in \mathbf{Q},\ a \notin \mathbf{Z},\ b \neq 0.$$

This equation has no solution $y \in \mathbf{Q}(z)$. The aim is to show that there are infinitely many primes $p$ such that the equation has no solution in $\mathbf{F}_p(z)$. For $p \equiv 3$ modulo 4, the operator $L : \mathbf{F}_p(z) \to \mathbf{F}_p(z)$, considered in 3.2, is bijective. Thus the only primes that interest us are $p \equiv 1$ modulo 4. The homogeneous equation $y' = ((az + b)/(z^2 + 1))y$ has a non zero solution $f \in F_p(z)$. For an element $d \in \mathbf{F}_p$ we write $\mathrm{Mod}[d, p]$ for its representative in $\{0, 1, \ldots, p-1\}$. For con-

venience we write $i$, for the element of $\mathbf{F}_p$ with $i^2 = -1$ and $\mathrm{Mod}[i,p] < p/2$. In the field $\mathbf{F}_p(z)$ \we have the identity

$$\frac{az+b}{z^2+1} = \frac{a/2+ib/2}{z+i} + \frac{a/2-ib/2}{z-i},$$

and thus

$$f = (z+i)^{\mathrm{Mod}[a/2+ib/2,p]}(z-i)^{\mathrm{Mod}[a/2-ib/2,p]}.$$

Variation of constants $y = Ff$ leads to the equation

$$F'(z^2+1)^p = (z+i)^{p-\mathrm{Mod}[a/2+ib/2,p]-1}(z-i)^{p-\mathrm{Mod}[a/2-ib/2,p]-1}.$$

Using the shift $z \mapsto z+i$, one easily sees that the last equation has a solution if and only if the degree of the right hand side is $\leq p-2$. The latter is equivalent with

$$\mathrm{Mod}[a/2+ib/2,p] + \mathrm{Mod}[a/2-ib/2,p] \geq p.$$

Thus we want to show that there are infinitely many primes $p \equiv 1$ modulo 4 such that the right hand side is $< p$.

For, say the case $a = 1/2$ and $b = 2$, this means that we have to find infinitely many primes $p \equiv 1$ modulo 4 with $\mathrm{Mod}[i,p] \leq (p-1)/4$. A computer experiment, run by a Ph.D. student W.R. Oudshoorn, showed that for the first $10^6$ primes $p$ with $p \equiv 1$ modulo 4, 'half' of the primes satisfy $\mathrm{Mod}[i,p] \leq (p-1)/4$. It was rather a surprise to learn from a Bourbaki talk (see [M]) that this computer experiment, and more generally the statement that there are infinitely many primes $p$ such that our equation has no solution in $\mathbf{F}_p(z)$, follows from a recent work of Duke, Friedlander, Iwaniec and Toth on Selberg's big sieve. The theorem is the following.

**Theorem 7.2.** *Let $f = x^2 + ax + b \in \mathbf{Q}[x]$ be an irreducible polynomial. Then the set*

$$\{\frac{v}{p} \in [0,1] \mid v \in \{0,1,\ldots,p-1\}, f(v) \equiv 0 \text{ modulo } p\}$$

*is uniformly distributed in* [0,1].

The method of the example and theorem 7.2 provide a proof of the following.

**Corollary 7.3.** *Conjecture 7.1 is true for equations $y' = ay + b$ where the denominator of $a \in \mathbf{Q}(z)^*$ is an irreducible polynomial of degree two.*

The method of the example can be extended to show that conjecture 7.1 for $y' = ay + b$, where $a$ has a denominator $f$ which is an irreducible polynomial of degree $> 2$, is equivalent with a weak form of theorem 7.2 for $f$ instead of a quadratic polynomial. Namely, the statement that suitable intervals in $[0,1]$ contain $\frac{v}{p}$ for infinitely many primes $p$.

REFERENCES


[A1] André Y. – Séries Gevrey de type arithmétiques. Institut de Mathématiques de Jussieu. Prépublication **119**, Mai 1997.

[A2] André Y. – Sur la conjecture des p-courbures de Grothendieck-Katz. Institut de Mathématiques de Jussieu. Prépublication **134**, Octobre 1997.

[BH] Beukers, F., G. Heckman – Monodromy for the hypergeometric function ${}_nF_{n-1}$. Invent. Math. **95**, 325–354 (1989).

[CC] Chudnovsky, D., G. Chudnovsky – Applications of Padé approximations to the Grothendieck conjecture on linear differential equations. In: Lect. Notes Math. **1135**, 52–100 (1985).

[E] Elkies, N. – The existence of infinitely many supersingular primes for every elliptic curve over **Q** – Invent. Math. **89**, 561–567 (1987).

[Ha] Haraoka, Y. – Finite monodromy of Pochhammer equation. Ann. Inst. Fourier, Grenoble 44,3, 767–810 (1994).

[Ho] Honda, T. – Algebraic differential equations. INDAM, Symp. Math. **XXIV**, 169–204 (1981).

[K1] Katz, N. – Algebraic solutions of differential equations ($p$-curvature and Hodge Filtration). Invent. Math. **18**, 1–118 (1972).

[K2] Katz, N. – Travaux de Dwork – Sém. Bourbaki, exp. 409, (1971-72), Lect. Notes. Math. **317** (1973).

[K3] Katz, N. – A conjecture in the arithmetic theory of differential equations. Bull. S.M.F. **110**, 203–239, corrig. Bull. S.M.F. **111**, 347–348 (1982).

[K4] Katz, N. – Rigid local systems. Annals of Math. Studies **139** (1996).

[M] Michel, Ph. – Progrès récents du crible et applications [d'après Duke, Fouvry, Friedlander, Iwaniec]. Sém. Bourbaki, exp. 842, (1997-98), Astérisque **252** (1998).

[P1] Put, M. van der – Differential equations in characteristic $p$. Compositio Math. **97**:227–251 (1995).

[P2] Put, M. van der – Reduction modulo $p$ of differential equations. Indag. Mathem. N.S., **7**(3), 367–387 (1996).


(Received April 2000)