Mathematische Zeitschrift manuscript No.
(will be inserted by the editor)

On Dwork's accessory parameter problem

Frits Beukers*

Utrecht University,e-mail: `beukers@math.uu.nl`

The date of receipt and acceptance will be inserted by the editor –

Abstract We study the question which ordinary second order linear differential equation allows power series solutions whose p-adic radius of convergence is at least one, a question raised by B.Dwork. In particular we shall consider the case of Fuchsian equations with four singularities and local exponent differences 0.

Key words accessory parameter–p-adic solution

1 Introduction

Let $P \in \mathbb{C}[z]$ be a monic quadratic polynomial with non-zero discriminant and $P(0) \neq 0$. Let $\lambda \in \mathbb{C}$. Consider the linear differential equation

$$zP(z)\frac{d^2u}{dz^2} + (zP(z))'\frac{du}{dz} + (z-\lambda)u = 0 \tag{1}$$

Note that this is the general shape of a Fuchsian differential equation on $\mathbb{P}^1$ with singularities in four points, including ∞, having local exponents $0, 0$ at the finite points and $1, 1$ at ∞. By scaling z if necessary we can assume that P has the form $P(z) = z^2 + az - 1$. Suppose we want to solve (1) by a power series expansion $u(z) = \sum_{n \geq 0} u_n z^n$. We then obtain the recursion relation

$$(n+1)^2 u_{n+1} = (an(n+1) - \lambda)u_n + n^2 u_{n-1} \quad (n \geq 1), \qquad u_1 = -\lambda u_0 \tag{2}$$

for the coefficients u_n. Without loss of generality we normalise to the case $u_0 = 1$.

* Part of this work was supported by EPSRC grant L99920

When $a=0,\lambda=0$ we obtain the recurrence

$$(n+1)^2u_{n+1}=n^2u_{n-1}$$

having the solution $u_{2n}=\binom{2n}{n}^2/16^n,\ u_{2n+1}=0$. Note that this solution consists of rational numbers which contain only 2's in the denominator. We call such numbers S-integers, where $S=\{2\}$. More, generally, letting S be any finite set of primes $p_1,\ldots,p_r$, the ring of rational numbers having only products of the p_i as denominator is called the ring of S-integers. Notation: $\mathbb{Z}_S$.

When $a=11,\lambda=-3$ we obtain the famous recurrence found by R.Apéry in 1978,

$$(n+1)^2u_{n+1}=(11n^2+11n+3)u_n+n^2u_{n-1}$$

having the solution $u_n=\sum_{k=0}^n\binom{n}{k}^2\binom{n+k}{k}$ in integers. Observe that in the recursion (2) we divide by $(n+1)^2$ at every step. So on would expect the denominator of u_n to grow like $(n!)^2$. This is what usually happens. However, for some choices of a,λ the u_n turn out to be S-integral for a given set of primes S. It is hopefully clear that the two above examples are quite exceptional in that they have S-integral solutions for some set S. By way of illustration we show at the very end of the paper that the only integer $\lambda\in\mathbb{Z}$ for which the recurrence $(n+1)^2u_{n+1}=(11n^2+11n-\lambda)u_n+n^2u_{n-1}$ has an integral solution, is $\lambda=-3$. This case corresponds to Apéry's above mentioned recurrence.

The main question would be the following

Question 1. Let S be a finite set of primes. Given $a\in\mathbb{Q}$, for which $\lambda\in\mathbb{Q}$ does (2) have a solution $u_0,u_1,\ldots\in\mathbb{Z}_S$?

Or, more generally over the algebraic numbers,

Question 2. Let S be a finite set of primes and denote by $\mathcal{O}_S$ the set of algebraic numbers that are integral outside the places above S. Given $a\in\overline{\mathbb{Q}}$, for which $\lambda\in\overline{\mathbb{Q}}$ does (2) have a solution $u_0,u_1,\ldots\in\mathcal{O}_S$?

Questions of this type have been addressed frequently in the work of B. Dwork, see [6, section 7],[?], [8]. Dwork's motivation for looking at this problem is a conjecture of Bombieri and Dwork which states that differential equations with an arithmetically well-behaved basis of solutions, should arise as factors of a Gauss-Manin system. Integrality of the coefficient is an example of being well-behaved. Other (not necessarily equivalent) descriptions are, having a basis of G-function solutions (see [1]) or nilpotent p-curvature for almost all primes p (see the references to Dwork's work). Beside this interest in the arithmetic of linear differential equations Questions 1 and 2 are also of importance to the construction of irrationality proofs, as exemplified by Apéry's recurrence. Recently, integrality questions have also been connected with problems in mirror-symmetry (see [13]).

Amused by Question 1 Don Zagier has carried out a large search for recurrences of the form,

$$(n+1)^2 u_{n+1} - An(n+1)u_n + Bn^2 u_{n-1} = \lambda u_n, \qquad u_0 = 1, u_1 = \lambda$$

where A, B are given rational integers. Note that this recursion is slightly different from (2) in that B need not be -1 here. For a search in the domain of rational integers $|A| \le 250, 0 \le u_1 \le 100, |u_2| \le 1000$ he found 36 recurrences which allow an integral solution u_n. Of these, only 7 satisfied the additional condition $B(A^2 - 4B) \neq 0$. This corresponds to the fact that the corresponding linear differential equation has exactly four singularities. Here is their list,

case#	A	B	λ	singular points
#1	0	-16	0	$1/4, -1/4, 0, \infty$
#2	7	-8	2	$-1, 1/8, 0, \infty$
#3	9	27	3	$(3 \pm \sqrt{-3})/18, 0, \infty$
#4	10	9	3	$1, 1/9, 0, \infty$
#5	11	-1	3	$(11 \pm 5\sqrt{5})/2, 0, \infty$
#6	12	32	4	$0, 1/4, 1/8, \infty$
#7	17	72	6	$1/8, 1/9, 0, \infty$

The singular points in this table are the singular points corresponding to the linear differential equation. Notice that the set of singularities of cases #2,#4 and #7 are equivalent via Möbius transformations. It turns out that the differential equation are also equivalent with respect to these transformations. The same remark holds for the cases #1 and #6. One may conjecture that up to the transformation $u_n \to c^n u_n$ these are the only cases where we find integral solutions for the recurrence. It has been pointed out by Zagier that these cases are closely related to the theory of classical modular forms.

In a similar vein one may also note that in these examples the differential equations are a pullback of a hypergeometric equation by a rational function. It is a finite amount of work to compute all Fuchsian differential equationsof the form (1) which are rational pullback of a hypergeometric equation. It turns out that the hypergeometric equation can always be taken with parameters $\alpha = 1/12, \beta = 5/12, \gamma = 1$. Here are the results, up to equivalence after Möbius transformations in z,

Case A: $(z^3 - z)y'' + (3z^2 - 1)y' + zy = 0$

Solution:

$$b(z)^{1/4} {}_2F_1 \left(\begin{matrix} 1/12 \; 5/12 \\ 1 \end{matrix} \middle| \frac{27z^8(1-z^2)}{1024 b(z)^3} \right)$$

where $b(z) = 1 - z^2 + z^4/16$.

Case B: $(z^3 - z)y'' + (3z^2 - 1)y' + zy = 0$

Solution:

$$b(z)^{1/4} {}_2F_1 \left(\begin{matrix} 1/12 \; 5/12 \\ 1 \end{matrix} \middle| \frac{27z^4(1-z^2)^2}{4 b(z)^3} \right)$$

where $b(z) = 1 - z^2 + z^4/16$.

Case C: $z(z-1)(8z+1)y'' + (24z^2 - 14z - 1)y' + (8z-2)y = 0$
Solution:

$$b(z)^{1/4}{}_2F_1\left(\begin{matrix}1/12\ 5/12\\ 1\end{matrix}\,\middle|\,\frac{1728z^6(z-1)^2(1+8z)}{b(z)^3}\right)$$

where $b(z) = 1 + 8z - 16z^3 + 16z^4$.

Case D: $z(z^2+11z-1)y'' + (3z^2+22z-1)y' + (z+3)y = 0$
Solution:

$$b(z)^{1/4}{}_2F_1\left(\begin{matrix}1/12\ 5/12\\ 1\end{matrix}\,\middle|\,\frac{1728z^5(1-11z-z^2)}{b(z)^3}\right)$$

where $b(z) = 1 - 12z + 14z^2 + 12z^3 + z^4$.

Case E: $z(3z^2-3z+1)y'' + (3z-1)^2y' + (3z-1)y = 0$
Solution:

$$b(z)^{1/4}{}_2F_1\left(\begin{matrix}1/12\ 5/12\\ 1\end{matrix}\,\middle|\,\frac{-64z^3(1-3z+3z^2)^3}{b(z)^3}\right)$$

where $b(z) = (1-z)(1-3z+3z^2-9z^3)$

Case F: $z(3z^2-3z+1)y'' + (3z-1)^2y' + (3z-1)y = 0$
Solution:

$$b(z)^{1/4}{}_2F_1\left(\begin{matrix}1/12\ 5/12\\ 1\end{matrix}\,\middle|\,\frac{-64z^9(1-3z+3z^2)}{729b(z)^3}\right)$$

where $b(z) = (1-z)(1-3*z+3*z^2-z^3/9)$.

Note that we find four different differential equations, which corresponds precisely to Zagier's list modulo a simple Möbius transformation in z. The six rational pullback functions that we have written down correspond precisely to the j-invariants of the six stable families of elliptic curves over $\mathbb{P}^1$ with four singularities. In [3] one can find this complete list. The reason that some of the corresponding Picard-Fuchs coincide, such A with B and E with F, is that the corresponding families of elliptic curves are modular with modular groups that are conjugate in $SL(2,\mathbb{R})$.

One may suspect that the full list of positive answers to Question 2 is provided by our list of four differential equations and their Möbius transforms in z. But we seem to be very far from proving this.

Since the above mentioned global questions seem so difficult to deal with we propose in this paper a local approach. Fix a prime number p and let k_p be the maximal unramified extension of $\mathbb{Q}_p$. Let $\mathbb{K}_p$ be its completion and let $\Omega_p = \{a \in \mathbb{K}_p \mid |a|_p \le 1\}$ be its ring of integers. The maximal ideal is generated by p and the quotient field $\Omega_p(\mathrm{mod}\ p)$ is simply $\overline{\mathbb{F}}_p$. Let $B_p \subset \mathbb{K}_p[[z]]$ be the set of power series uniformly bounded in the open unit disc, that is,

$$\sum_{n\ge 0} u_n z^n \in B_p \iff \exists\, b:\ |u_n|_p \le b \text{ for all } n \ge 0$$

By U_p we denote the set of powerseries in $\mathbb{K}_p[[z]]$ with p-adic radius of convergence at least 1. Notice that $\Omega_p[[z]] \subset B_p \subset U_p$. Note also that B_p, U_p are $\mathbb{K}_p$-vector spaces. To make our methods work we have to assume that $a \in \Omega_p$ and the discriminant of P is a unit in Ω_p. We now ask the following local question,

Question 3. Given $a \in \Omega_p$ with $a^2+4 \in \Omega_p^\times$. For which $\lambda \in \mathbb{K}_p$ does the equation (1) have a solution in B_p, or in U_p ?

In [9], at the end of the introduction, problems dealing with accessory parameters are considered to be among the main problems in the theory of p-adic differential equations. It is for this reason that we refer to Question 3, and also its generalisation to more general differential equations, as *Dwork's accessory parameter problem.*

We can also view Question 3 as an eigenvalue problem. Consider the linear differential operator $L = zPD^2 + (zP)'D + z$, where $D = \frac{d}{dz}$, an an operator on B_p or U_p. Then Question 3 simply comes down to the eigenvalue problem

$$Lu = \lambda u, \qquad u \in U_p \quad \text{or} \quad u \in B_p. \tag{3}$$

Before we state the theorems of this paper we like to sketch the observations concerning recursion (2) that have led to these theorems. When we look at recursion (2) one may expect factors p in the denominator whenever we divide by $(n+1)^2$ containing a factor p. However, it turns out that things are not so bad. Suppose we have found a value of λ for which $u_0, u_1, \ldots, u_{p^k-1} \in \Omega_p$. The computation of u_{p^k} via (2) may introduce denominators p or not. Suppose not. Then, very surprisingly, it turns out that denominators p will not show up for $n = p^k, p^k+1, \ldots, p^{k+1}-1$ even though we divided by powers of p at several stages during the recurrence. This is proved in Proposition 2.

Suppose, on the other hand that $u_{p^k} \notin \Omega_p$. Then it is shown in Proposition 1 that $|u_{mp^k}|_p \geq |u_{p^k}|_p^m$ for all $m \geq 1$. Hence the p-adic radius of convergence of the power series $u(z)$ is strictly less than 1. All this explains the following theorem.

Theorem 1. *Suppose there exist $u(z) \in U_p$ and $\lambda \in \mathbb{K}_p$ such that $Lu = \lambda u$ and $u(0) = 1$. Then $\lambda \in \Omega_p$ and $u \in \Omega_p[[z]]$.*

This Theorem is a consequence of a theorem by Adolphson, Dwork and Sperber [2, p 249], but here we give a self-contained proof.

We remark here very explicitly that Theorem 1 does not generalise to differential equations whose local exponent differences are different from zero.

To describe the second theorem we first consider L as a linear operator on $\overline{\mathbb{F}}_p[z]$. In section 2 we see that it maps the space of polynomials of degree $< p$ to itself. If the eigenvalue problem $Lu = \lambda u$ on this space has p distinct eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_p \in \overline{\mathbb{F}}_p$ we shall say that the eigenvalue problem is *non-degenerate mod p*. This is what will be assumed throughout the paper. When this is the case, there exist p distinct eigenpolynomials $f_1, f_2, \ldots, f_p \in \overline{\mathbb{F}}_p[z]$ of degree $< p$ which we normalise by $f_i(0) = 1$. We can now state our second theorem.

Theorem 2. *Assume that the eigenvalue problem $Lu \equiv \lambda u (\mathrm{mod}\ p)$ is non-degenerate. Then there is a one-to-one correspondence between the set of all $u \in \Omega_p[[z]], \lambda \in \Omega_p$ such that $Lu = \lambda u$ and the set of all sequences of indices $i_0, i_1, i_2, \ldots \in \{1, \ldots, p\}$. The correspondence is given by*

$$u(z) \equiv f_{i_0}(z) f_{i_1}(z)^p f_{i_2}(z)^{p^2} \cdots f_{i_k}(z)^{p^k} \cdots (\mathrm{mod}\ p)$$

Moreover, $\lambda_{i_k}^{p^k}$ is precisely minus the coefficient of z^{p^k} in u considered mod p.

Finally we describe the shape of the spectrum of the operator L on the spaces U_p, B_p or, equivalently, $\Omega_p[[z]]$. Note that for any $\lambda \in \Omega_p$ there exists a unique solution $u_\lambda(z) \in \mathbb{K}_p[[z]]$ with $u_\lambda(0) = 1$ where the suffix λ indicates the dependence of u on λ. We now like to find λ such that $u_\lambda \in \Omega_p[[z]]$. To do this we follow our recursion (2). Since $\lambda \in \Omega_p$ we have that $u_\lambda(n) \in \Omega_p$ for $n = 0, 1, \ldots, p-1$, where $u_\lambda(n)$ denotes the n-th coefficient of u_λ. We easily see that $u_\lambda(p)$ is a polynomial of degree p in λ with integral coefficients, divided by p^2. Hence integrality of $u_\lambda(p)$ puts a mod p^2 constraint on a degree p polynomial in λ. Assuming the non-degeneracy condition we find p residue classes mod p^2 of values of λ for which $u_\lambda(p) \in \Omega_p$. Choose such a class and denote it by $\lambda_0 + p^2\beta$ with $\beta \in \Omega_p$. We can now continue our recurrence, and as we explained above, we will not meet any trouble until we hit $u_\lambda(p^2)$. Proposition 3 then tells us that $u_\lambda(p^2)$ equals modulo Ω_p a p-th degree polynomial in $\Omega_p[\beta]/p^2$. The non-degeneracy condition will give us p congruence classes mod p^2 of values of β which will make $u_\lambda(p^2)$ integral. Choose such a class and again continue. This process can be carried out arbitrarily far and clarifies more or less our third theorem.

Theorem 3. *We assume the non-degeneracy condition described above. Consider a directed tree graph in which to every node there correspond p outgoing edges and 1 incoming edge, except at the root where we have only p outgoing edges. To every node we can associate a number in Ω_p such that the following property holds. There is a one to one correspondence between eigenvalues λ of $Lu = \lambda u,\ u \in U_p$ and infinite directed paths starting at the root. This correspondence is given by*

$$\lambda = \lambda_0 + \lambda_1 p^2 + \lambda_2 p^4 + \cdots + \lambda_n p^{2n} + \cdots$$

where the numbers $\lambda_0, \lambda_1, \lambda_2, \ldots$ correspond to the nodes visited by the path excluding the root of the tree.
Moreover, if a is algebraic over $\mathbb{Q}_p$ then all eigenvalues of (3) lie in the same finite unramified extension of $\mathbb{Q}_p$.

In particular this theorem implies that our spectral problem has a Cantor-like set in Ω_p as a spectrum. To illustrate the last theorem we consider the example where $a = 0$ and $p = 3$. Consider the tree diagram in figure 1.

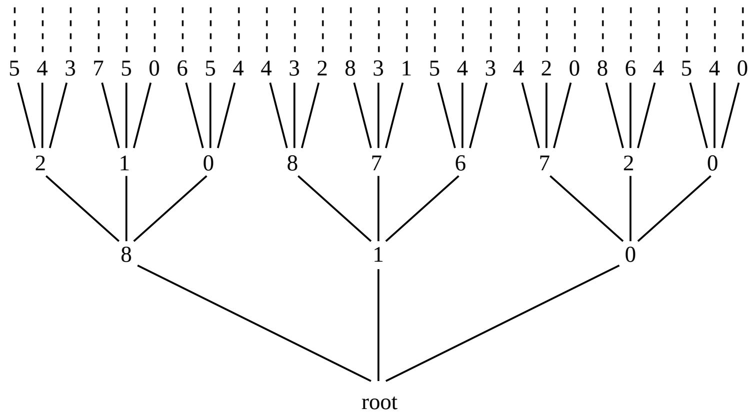

figure 1

Consider the path beginning at the root and visiting the nodes with numbered with $1, 6, 5, \ldots$. Then this path corresponds to the eigenvalue $\lambda = 1 + 6 \cdot 9 + 5 \cdot 9^2 + \cdots$ of the spectral problem (3) in the case when $a = 0$ and $p = 3$.
Cantor-like sets as spectra of operators have occured at a few places in the literature. A very nice example is associated to Hofstadter's butterfly, see [10]. nother reference can be found in a remarkable paper by the Chudnovsky's [5, Section 1.7]. It seems they have made extensive computations and observed Cantor-like spectra experimentally.
A question which we like to see solved in this matter is the following.

Question 4. Is there a continuous p to 1 map from Ω_p to itself which stabilises the set of eigenvalues? Presumably this would be connected to a better understanding of Frobenius actions on the set of eigenvalues.

Acknowledgements I would like to thank the Newton Institute of Mathematical Sciences in Cambridge (U.K.) for its hospitality, which enabled me to finish the work on this paper. I also like to thank Gilles Christol and Don Zagier for a number of valuable discussions which helped to shape the paper in its final form.

2 Considerations modulo p

We consider the differential equation (1) modulo p, hence $P = z^2 + az - 1$ with $a, \lambda \in \overline{\mathbb{F}}_p$. Given a we shall be interested in those values of λ for which there exists a solution $u \in \overline{\mathbb{F}}_p[[z]]$.

Lemma 1. *Suppose that (1) modulo p has a solution in $\overline{\mathbb{F}}_p[[z]]$. Then there is a unique polynomial solution $u \in \overline{\mathbb{F}}_p[[z]]$ such that $u(0) = 1$ and $\deg(u) < p$. Moreover, the full set of solutions in $\overline{\mathbb{F}}_p[[z]]$ is given by $\{Q(z^p)u(z) \mid Q(X) \in \overline{\mathbb{F}}_p[[X]]\}$.*

Proof. We shall exploit the fact that if y is a solution of (1), then so is $z^p y$, since z^p is constant with respect to differentiation in characteristic p. Let $v = \sum_{n \ge A} v_n z^n \in \overline{\mathbb{F}}_p[[z]]$ with $v_A \ne 0$ be a solution of (1). Since the v_n also satisfy recursion (2) we see that, taking $n = A - 1$, $A^2 v_A = 0$. Since $v_A \ne 0$ we conclude that $A \equiv 0 (\mathrm{mod}\ p)$. Hence $z^{-A} v$ is a powerseries solution with a non-zero constant term. We denote this solution again by v and may assume that $v(0) = 1$. Consider now recurrence (2) for $n = p-1, p$

$$\begin{aligned} 0^2 v_p &= -\lambda v_{p-1} + v_{p-2} \\ v_{p+1} &= -\lambda v_p + 0^2 v_{p-1} \end{aligned}$$

From this recurrence we see that $v_0, v_1, \ldots, v_{p-1}, 0, 0, \ldots$ is also a solution of (2). Hence $\sum_{n=0}^{p-1} v_n z^n$ is a polynomial solution of (1) of degree $< p$ and constant term 1. Call it $u(z)$. Let $v(z)$ be any solution in $\overline{\mathbb{F}}_p[[z]]$. Then $v(z) - v(0)u(z)$ is another such solution and by the arguments above it is divisible by a power of z^p. Divide by this power to obtain a new powerseries solution and repeat the process. In this way we see that the full set of powerseries solutions is given by $\{Q(z^p)u(z) \mid Q(X) \in \overline{\mathbb{F}}_p[[X]]\}$. **qed**

The above lemma shows that finding powerseries solutions of (1) in characteristic p comes down to finding polynomial solutions of degree $< p$. In this respect we make a few remarks. Denote the linear operator $zP(d/dz)^2 + (zP)'(d/dz) + z$ by L. Now notice that $L(z^k)$ is a polynomial of degree $\le k+1$ for all k and in particular,

$$\begin{aligned} L(z^{p-1}) &= (p-1)(p-2)z^p + 3(p-1)z^p + z^p + \text{terms of degree } < p \\ &= p^2 z^p + \text{terms of degree } < p \end{aligned}$$

Hence, in characteristic p the operator L maps polynomials of degree $< p$ to itself. Denote by V the $\overline{\mathbb{F}}_p$-vector space of polynomials in $\overline{\mathbb{F}}_p[z]$ of degree $< p$. Then $L : V \to V$.

Writing down the eigenvalue equation for L as an operator on V is easy. We consider λ as an indeterminate and follow the recurrence

$$u_1 = -\lambda u_0 \tag{4}$$

$$(n+1)^2 u_{n+1} = (an(n+1) - \lambda)u_n + n^2 u_{n-1} \qquad 1 \le n < p-1 \tag{5}$$

and define

$$F(\lambda) = (a(p-1)p - \lambda)u_{p-1} + (p-1)^2 u_{p-2}. \tag{6}$$

Note that $F(\lambda)$ is a polynomial of degree p in λ. The condition $F(\lambda) = 0$ gives us the eigenvalue equation. This is precisely the eigenvalue problem modulo p alluded to in the paragraph before Theorem 2 in the Introduction.

Lemma 2. *Consider the differential equation*

$$qy'' + q'y' + (z-\lambda)y = 0 \tag{7}$$

with $q \in \overline{\mathbb{F}}_p[z], \lambda \in \overline{\mathbb{F}}_p$ with q monic and cubic with non-zero discriminant. Suppose that the equation has a solution $u \in \overline{\mathbb{F}}_p[z]$ of degree $< p$. We assume that the leading coefficient of u is 1. Then, for any zero α of q we have $u(\alpha)^2 = q'(\alpha)^{p-1}$. Moreover, u has exact degree $p-1$.

Proof. Without loss of generality we may assume that $\alpha = 0$, i.e. $q(0) = 0$. Note that $T : z \mapsto q'(0)/z$ has the property that $q(T(z)) = q'(0)^2 q(z)/z^4$. In other words, T permutes the singularities of (7). Take the pullback of (7) by T, i.e. replace z by $q'(0)/z$ in (7), and then replace y by $z^{-1}y$. We obtain a new differential equation which turns out to be the same as (7). This can be checked by straightforward computation. As a consequence we find that $z^{-1}u(T(z))$ is also a solution of (7). Hence $z^{p-1}u(T(z))$ is a polynomial solution of (7) of degree $< p$ and by the uniqueness of u we find that there exists μ such that $z^{p-1}u(T(z)) = \mu u(z)$. Since T is an involution, we find that $\mu^2 = q'(0)^{p-1}$. Moreover, by taking $z = \infty$ in $u(q'(0)/z) = \mu z^{1-p} u(z)$ we get that $u(0) = \mu$ since the leading coefficient of u is 1. Hence $u(0)^2 = \mu^2 = q'(0)^{p-1}$ as asserted **qed**

Corollary 1. *Consider the differential equation (1) mod p. Suppose that it has a solution $u \in \overline{\mathbb{F}}_p[z]$ of degree $p-1$ and assume $u(0) = 1$. Let $l(u)$ be the leading coefficient of u. Then $l(u) = \pm 1$.*

Proof. Apply the previous Lemma to $q(z) = zP(z)$, $\alpha = 0$ and the solution $u/l(u)$. We find that $(u(0)/l(u))^2 = 1$. Since $u(0) = 1$ our Corollary follows. **qed**

Lemma 3. *Suppose that equation (7) has a polynomial solution u of degree $< p$. Assume that u has leading coefficient 1. Then,*

1. *$q(\alpha) = 0 \Rightarrow u(\alpha) \neq 0$*
2. *u has only simple zeros.*
3. *$D^{p-1}(1/qu^2) = -1/q^p$ where $D = d/dz$.*

Proof. Suppose $q(\alpha) = 0$. After the substitution $z \to z + \alpha$ we may assume $\alpha = 0$. From Lemma 1 we then see that $u(0) \neq 0$.
Suppose that there is α such that $q(\alpha) \neq 0$ and $u(\alpha) = u'(\alpha) = 0$. Then, by the use of (7) we recursively get that $u''(\alpha) = \cdots = u^{(p-1)}(\alpha) = 0$. Hence $u(z) \equiv 0$.
To show the third part we determine the partial fraction expansion of $1/qu^2$. Let Q be the set of zeros of q and U the set of zeros of u. Then there exist $q_\alpha, a_\beta, b_\beta \in \overline{\mathbb{F}}_p$ such that

$$\frac{1}{qu^2} = \sum_{\alpha \in Q} \frac{q_\alpha}{z-\alpha} + \sum_{\beta \in U} \frac{a_\beta}{(z-\beta)^2} + \frac{b_\beta}{z-\beta}$$

Differentiate $p-1$ times. Then, using $(p-1)! \equiv -1 \pmod p$ (Wilson's theorem),

$$D^{p-1}\left(\frac{1}{qu^2}\right) = -\sum_{\alpha\in Q}\frac{q_\alpha}{(z-\alpha)^p} - \sum_{\beta\in U}\frac{b_\beta}{(z-\beta)^p}$$

To determine b_β we write

$$\begin{aligned} qu^2 &= (q(\beta)+q'(\beta)(z-\beta)+\ldots)(u'(\beta)(z-\beta)+u''(\beta)(z-\beta)^2/2+\ldots)^2 \\ &= q(\beta)u'(\beta)^2(z-\beta)^2(1+\frac{q'(\beta)}{q(\beta)}(z-\beta)+\ldots)(1+\frac{u''(\beta)}{u'(\beta)}(z-\beta)+\ldots) \\ &= q(\beta)u'(\beta)^2(z-\beta)^2(1+\frac{q'(\beta)u'(\beta)+q(\beta)u''(\beta)}{q(\beta)u'(\beta)}(z-\beta)+\ldots) \end{aligned}$$

Using (7) with $z=\beta$ and $u(\beta)=0$ we see that $q'(\beta)u'(\beta)+q(\beta)u''(\beta)=0$. Hence

$$\frac{1}{qu^2} = \frac{1}{q(\beta)u'(\beta)^2}\frac{1}{(z-\beta)^2}(1+O((z-\beta)^2))$$

So we conclude that $b_\beta = 0$ for all $\beta\in U$.
Finally, $q_\alpha = 1/(q'(\alpha)u(\alpha)^2)$ and using Lemma 2 this implies $q_\alpha = 1/q'(\alpha)^p$. Hence

$$D^{(p-1)}\frac{1}{qu^2} = -\sum_{\alpha\in Q}\frac{1}{q'(\alpha)^p(z-\alpha)^p} = -\frac{1}{q^p}.$$

qed

Corollary 2. *Let assumptions be as in the previous Lemma and suppose in addition that $q = zP(z)$, where P is quadratic and $P(0)=1$. Define the operator $V_p : \overline{\mathbb{F}}_p[[z]] \to \overline{\mathbb{F}}_p[[z]]$ by $V_p(\sum_{k\ge0} g_k z^k) = (\sum_{k\ge0} g_{kp} z^k)$. For any $g = \sum_{k\ge0} g_k z^k \in \overline{\mathbb{F}}_p[[z]]$ denote by g^σ the power series $g^\sigma = \sum_{k\ge0} g_k^p z^k$. Then,*

$$V_p\left(\frac{1}{Pu^2}\right) = \frac{1}{P^\sigma}$$

Proof. By Wilson's theorem we see that for every $g\in\overline{\mathbb{F}}_p[[z]]$ we have

$$D^{p-1}\left(\frac{g}{z}\right) = -\frac{(V_p g)(z^p)}{z^p}$$

We apply this observation to $g = 1/Pu^2$ and use the previous Lemma to obtain

$$\frac{1}{z^p P(z)^p} = \frac{(V_p(1/Pu^2))(z^p)}{z^p}$$

Multiply by z^p and observe that $P(z)^p = P^\sigma(z^p)$ to find $1/P^\sigma(z^p) = (V_p(1/Pu^2))(z^p)$. Our Corollary follows after we replace z^p by z. **qed**

Corollary 3. *Let $f_1, f_2, \ldots, f_p$ be the normalised eigenpolynomials of the eigenvalue problem $Lu \equiv \lambda u (\bmod p)$. Then, for any finite sequence of indices $i_0, i_1, \ldots, i_{k-1}$ we have*

$$(V_p)^k \left(\frac{1}{P(f_{i_0}(z) f_{i_1}(z)^p \cdots f_{i_{k-1}}(z)^{p^{k-1}})^2} \right) \equiv \frac{1}{P^{\sigma^k}} (\bmod p).$$

Proof. Apply V_p to

$$\frac{1}{P(f_{i_0} f_{i_1}^p \cdots f_{i_{k-1}}^{p^{k-1}})^2} (\bmod p).$$

Use Corollary 2 with $u = f_{i_0}$ to obtain

$$\begin{aligned} V_p \left(\frac{1}{P(f_{i_0} \cdots f_{i_{k-1}}^{p^{k-1}})^2} \right) &\equiv V_p \left(\frac{1}{P f_{i_0}^2} \right) \frac{1}{(f_{i_1}^\sigma (f_{i_2}^\sigma)^p \cdots (f_{i_{k-1}}^\sigma)^{p^{k-2}})^2} (\bmod p) \\ &\equiv \frac{1}{P^\sigma(z)(f_{i_1}^\sigma (f_{i_2}^\sigma)^p \cdots (f_{i_{k-1}}^\sigma)^{p^{k-1}})^2} (\bmod p). \end{aligned}$$

After repeating this operation k times we find our Corollary. **qed**

3 Proof of the main theorems

Let L be the differential operator $L = zPD^2 + (zP)'D + z$. Given any $\lambda \in \Omega_p$ there exists a power series $u_\lambda \in \mathbb{K}_p[[z]]$ such that $(L - \lambda)u_\lambda = 0$ and $u_\lambda(0) = 1$. The coefficients of u_λ are of course determined by the recursion (2). We denote the n-th coefficient of u_λ by $u_\lambda(n)$. For any $k \geq 0$ we denote by $u_{k,\lambda}$ the truncation polynomial

$$u_{k,\lambda} = \sum_{n<p^k} u_\lambda(n) z^n.$$

We note that, after a short computation,

$$(L - \lambda)u_{k,\lambda} = p^{2k}(u_\lambda(p^k) z^{p^k - 1} + u_\lambda(p^k - 1) z^{p^k}). \tag{8}$$

Finally we introduce the power series $g_{k,\lambda} \in \mathbb{K}_p[[z]]$ as the quotient $u_\lambda / u_{k,\lambda}$. If the dependence of $u_\lambda, u_{k,\lambda}, g_{k,\lambda}$ on λ is not relevant or if notations tend to become cumbersome we usually drop the suffix λ from the notation.

Lemma 4. *Let u, u_k, g_k be as above. Then*

$$g_k = 1 - \int_0^z \frac{1}{P u_k^2 z} \int_0^z g_k u_k (L - \lambda) u_k \, dz. \tag{9}$$

Proof. From $(L-\lambda)u=0$ we derive $(L-\lambda)(u_k g_k)=0$ and hence

$$2zPu_k'g_k' + zPu_k g_k'' + (zP)'u_k g_k' + g_k(L-\lambda)u_k = 0.$$

Multiply by u_k and we get

$$(zPu_k^2 g_k')' = -u_k g_k (L-\lambda)u_k$$

Hence

$$zg_k' = -\frac{1}{Pu_k^2}\int_0^z u_k g_k (L-\lambda)u_k dz$$

After divison by z and again an integration from 0 to z we obtain our functional equation for g_k. **qed**

For the proof of our theorems we introduce some more notation. First of all we note, using (8), that $u_k(L-\lambda)u_k/p^{2k}$ has the form

$$v_{2p^k-1}z^{2p^k-1} + \cdots + v_{p^k-1}z^{p^k-1}$$

where, in particular, $v_{2p^k-1} = u(p^k-1)^2$ and $v_{p^k-1} = u(p^k)$.
We expand $1/Pu_k^2$ as a power series

$$\frac{1}{Pu_k^2} = 1 + b_1 z + b_2 z^2 + \cdots \in \mathbb{K}_p[[z]]$$

Note that the b_i are in Ω_p if $u_k \in \Omega_p[z]$. Let $g_k(z) = 1+\gamma_1 z+\gamma_2 z^2+\gamma_3 z^3+\cdots$. To avoid cluttering of indices we have suppressed the dependence of the γ_i on k. Since we assume k to be fixed throughout the proofs, this is no serious problem.
The functional equation (9) now implies the following recurrence for the coefficients γ_n,

$$\gamma_n = -\frac{p^{2k}}{n}\sum_{r+s+t=n-1} b_r \frac{v_s\gamma_t}{s+t+1} \tag{10}$$

Proposition 1. *Let $k \ge 0$ and suppose $u(n) \in \Omega_p$ for $n = 0,1,\ldots,p^k-1$ and $R = |u(p^k)|_p > 1$. Then, for any $m \ge 1$ we have*

1. $|u(mp^k)|_p = R^m/|m!|_p^2$
2. $|u(n)|_p < R^m/|m!|_p^2$ *for all* $n < mp^k$.

Proof. We use the recursion (10) to show the inequalities for the coefficients γ_n instead of $u(n)$. Using the relation

$$u(z) = \sum_{n=0}^{\infty} u(n)z^n = u_k(z)g_k(z) = u_k(z)(1+\gamma_1 z + \gamma_2 z^2 + \cdots)$$

the inequalities for the $u(n)$ follow.
We proceed by induction on m. For $m=1$ the statement is clear. Now suppose that statements (1) and (2) are proved for $m = 1,2,\ldots,M$. Let n be such that $Mp^k < n \le (M+1)p^k$. Consider recurrence (10). We will

show that each term on the right hand side with $t < Mp^k$ has absolute value strictly less than $R^{M+1}/|(M+1)!|_p^2$. Note that we have trivially

$$\left|\frac{p^{2k}}{n}\right|_p \leq \left|\frac{p^k}{M+1}\right|_p .$$

Suppose first that t is not divisible by p^k and $t < Mp^k$. Choose L such that $(L-1)p^k < t < Lp^k$. Then $\min_{s=p^k-1,\ldots,2p^k-1} |s+t+1|_p = |(L+1)p^k|_p$. Hence

$$\begin{aligned}\left|\frac{p^{2k}}{n} b_r \frac{v_s \gamma_t}{s+t+1}\right|_p &< R\left|\frac{p^k}{M+1}\frac{\gamma_{Lp^k}}{(L+1)p^k}\right|_p = \frac{R^{L+1}}{|(M+1)(L+1)|_p}\frac{1}{|L!|_p^2}\\ &\leq \frac{R^{M+1}}{|(M+1)!|_p^2}.\end{aligned}$$

In the estimate we have used the inequalities $|b_r|_p \leq 1$, $|v_s|_p \leq R$ plus the fact that $|\gamma_t| < |\gamma_{Lp^k}| = R^L/|L!|_p^2$, which follows from our induction hypothesis.
Suppose now that $t = Lp^k$ for some $L \leq M-1$. Then

$$\min_{s=p^k-1,\ldots,2p^k-1} |s+t+1|_p = \min(|(L+1)p^k|_p, |(L+2)p^k|_p) \geq |(L+1)(L+2)p^k|_p .$$

Hence

$$\begin{aligned}\left|\frac{p^k}{M+1} b_r \frac{v_s \gamma_t}{s+t+1}\right|_p &\leq \left|\frac{p^k}{M+1}\frac{1}{(L+1)(L+2)p^k}\right|_p \frac{R^{L+1}}{|L!|_p^2}\\ &\leq \frac{R^{L+1}}{|(M+1)!|_p^2} < \frac{R^{M+1}}{|(M+1)!|_p^2}.\end{aligned}$$

So we have shown that each term on the right of (10) with $t < Mp^k$ has absolute value $< R^{M+1}/|(M+1)!|_p^2$.
Note that if $n < (M+1)p^k$ the inequalities $s+t < n$ and $s \geq p^k - 1$ imply that $t < Mp^k$. Hence $|\gamma_n|_p < R^{M+1}/|(M+1)!|_p^2$, as asserted in part (2).
If $n = (M+1)p^k$ there is only one term with $t \geq Mp^k$ namely the term with $r = 0, s = p^k - 1$ and $t = Mp^k$. A simple computation shows that it has absolute value $R^{M+1}/|(M+1)!|_p^2$, which shows part (1) of our Proposition.
qed

Proposition 2. *Suppose that the eigenvalue problem $Lu \equiv \lambda u (\mathrm{mod}\ p)$ has p distinct eigenvalues in $\lambda_1, \lambda_2, \ldots, \lambda_p \in \overline{\mathbb{F}}_p$. Let $f_1, f_2, \ldots, f_p$ be the corresponding normalised eigenpolynomials of degree $p-1$.*
Suppose we have $u(n) \in \Omega_p$ for $n = 0, 1, \ldots, p^k - 1$. Suppose in addition that $u(p^k) \in \Omega_p$. Then the following two properties hold,

1. *There exist indices $i_0, i_1, \ldots, i_{k-1}$ such that*

$$u_k(z) \equiv f_{i_0}(z) f_{i_1}(z)^p f_{i_2}(z)^{p^2} \cdots f_{i_{k-1}}(z)^{p^{k-1}} (\mathrm{mod}\ p).$$

   Moreover, $\lambda_{i_l}^{p^l} \equiv -u(p^l) (\mathrm{mod}\ p)$ for $0 \leq l < k$.

2. *We have $u(n) \in \Omega_p$ for $n = 0, 1, 2, \ldots, p^{k+1}-1$. Moreover the coefficients γ_n of $\gamma_k(z) = u(z)/u_k(z)$ are zero mod p if n is less than p^{k+1} and not divisible by p^k. The coefficients $G_m = \gamma_{mp^k}$ satisfy the partial recurrence*

$$(m+1)^2 G_{m+1} \equiv (a^{p^k} m(m+1) - \Lambda) G_m + m^2 G_{m-1} (\text{mod } p)$$

for $m = 1, 2, \ldots, p-2$ with initial values $G_0 = 1$, $G_1 \equiv -\Lambda$ and where $\Lambda \equiv -u(p^k)(\text{mod } p)$.

Proof. First we will show that part (2) is a consequence of part (1) for any $k \geq 1$. Then we prove part (1) by induction on $k = 1, 2, 3, \ldots$.
First of all we like to note that it follows from (1) that $u(p^k - 1) \equiv \pm 1(\text{mod } p)$. This follows from part (1) and Corollary 1 which tells us that $f_i(z)$ has leading coefficient ± 1 for every i.
Consider the recurrence (10) again. Note that by the assumption $u(p^k) \in \Omega_p$ we have that $v_s \in \Omega_p$ for all s. Whenever $n < p^{k+1}$ we see that $p^{2k}/n(s+t+1)$ is a p-adic integer. Hence by recursion, $\gamma_n \in \Omega_p$ for $0 \leq n < p^{k+1}$. As a consequence, $u(n) \in \Omega_p$ for $n = 0, 1, 2, \ldots, p^{k+1} - 1$. Furthermore, if n is not divisible by p^k then $p^{2k}/n(s+t+1)$ is always zero mod p. Hence $\gamma_n \equiv 0(\text{mod } p)$ for all $n < p^{k+1}$ not divisible by p^k.
We now derive a recursion relation for the numbers γ_{mp^k} modulo p with $m = 0, 1, 2, \ldots, p-1$.
Recursion (10) yields for all $m \geq 1$,

$$m\gamma_{mp^k} = -p^k \sum_{r+s+t=mp^k-1} b_r \frac{v_s \gamma_t}{s+t+1} \tag{11}$$

Now assume that also $m < p$. Note that a term on the right is zero modulo p if p^k does not divide $s+t+1$. Hence, in considerations modulo p only the terms with r of the form $r = \rho p^k$ are relevant,

$$m\gamma_{mp^k} \equiv -\sum_{\rho=0}^{m-1} b_{\rho p^k} \sum_{s+t+1=(m-\rho)p^k} \frac{v_s \gamma_t}{m-\rho} (\text{mod } p)$$

Now we use that $\gamma_t \equiv 0(\text{mod } p)$ unless $p^k | t$. Putting $t = \tau p^k$ and $s = \sigma p^k - 1$ we get

$$m\gamma_{mp^k} \equiv -\sum_{\rho=0}^{m-1} b_{\rho p^k} \sum_{\sigma+\tau=m-\rho} \frac{v_{\sigma p^k - 1} \gamma_{\tau p^k}}{m-\rho} \tag{12}$$

$$\equiv -\sum_{\rho=0}^{m-1} b_{\rho p^k} \left(\frac{-\Lambda \gamma_{(m-\rho-1)p^k} + \gamma_{(m-\rho-2)p^k}}{m-\rho} \right) (\text{mod } p) \tag{13}$$

In the latter congruence we used the fact that $v_{p^k-1} = u(p^k) = -\Lambda$ and $v_{2p^k-1} = u(p^k-1)^2 \equiv 1(\text{mod } p)$. Note that

$$\sum_{\rho \geq 0} b_{\rho p^k} z^r \equiv (V_p)^k \left(\frac{1}{P u_k^2} \right) (\text{mod } p)$$

Using the fact from part (1) that $u_k \equiv f_{i_0} \cdots f_{i_{k-1}}^{p^{k-1}} (\text{mod } p)$ and Corollary 3 we derive

$$\sum_{\rho \geq 0} b_{\rho p^k} z^r \equiv \frac{1}{P^{\sigma^k}} (\text{mod } p)$$

Write

$$G(z) = \sum_{r \geq 0} \gamma_{rp^k} z^r$$

Then (3) implies that

$$zP^{\sigma^k} G' \equiv \int_0^z (z - \Lambda) G dz (\text{mod } p, z^p)$$

After differentiation,

$$zP^\sigma G'' + (zP^\sigma)' G' + (z - \Lambda) G \equiv 0 (\text{mod } p, z^{p-1})$$

Hence the coefficients of G satisfy the partial recurrence mod p of assertion (2).
Let us now prove statement (1) using induction on $k \geq 1$. For $k = 1$ the statement is obviously true. Let us assume it is proved for $k = 1, 2, \ldots, K$. The induction hypothesis implies that $u(p^{K+1}) \in \Omega_p$. Hence $\gamma_{p^{K+1}} \in \Omega_p$. Given this, the left-hand side of (11) with $m = p$ is in Ω_p. On the right hand side all terms with $s + t + 1 < p^{k+1}$ are p-adically integral. Terms with $s + t + 1 = p^{K+1}$ are of the form $v_s \gamma_t / p$. Since $\gamma_t \equiv 0 (\text{mod } p)$ if t is not divisible by p^K we conclude that the sum of the remaining terms, that is $(v_{p^K - 1} G_{p-1} + v_{2p^K - 1} G_{p-2})/p$, is in Ω_p. Hence $-\Lambda G_{p-1} + G_{p-2} \equiv 0 (\text{mod } p)$. Using the formula (6) for eigenvalues of the mod p problem, we conclude that Λ is an eigenvalue of the eigenvalue problem $\tilde{L} u \equiv \Lambda u (\text{mod } p)$ where $\tilde{L}$ denotes the operator L with a replaced by a^{p^K}. Choose i_K such that $\lambda_{i_K}^{p^K} \equiv \Lambda (\text{mod } p)$. Then we see that

$$\gamma_K(z) \equiv (f_{i_K})^{\sigma^K} (z^{p^K}) (\text{mod } p, z^{p^{K+1}})$$

hence

$$u_{K+1}(z) \equiv u_k(z) (f_{i_K}(z))^{p^K} (\text{mod } p)$$

which completes our induction step. **qed**

Proposition 3. *Suppose that the eigenvalue problem* $Lu \equiv \lambda u (\text{mod } p)$ *has* p *distinct eigenvalues in* $\lambda_1, \lambda_2, \ldots, \lambda_p \in \overline{\mathbb{F}}_p$. *Let* $f_1, f_2, \ldots, f_p$ *be the corresponding normalised eigenpolynomials of degree* $p - 1$.
Let $k \geq 0$. *Let* $\lambda_0 \in \Omega_p$ *and denote the elements of the residue class* $\lambda_0 (\text{mod } p^{2k})$ *by* $\lambda = \lambda_0 + p^{2k} \beta$, $\beta \in \Omega_p$. *Suppose the following holds,*

1. $u_\lambda(n) \in \Omega_p$ *for* $n = 0, 1, \ldots, p^k$ *and all* $\beta \in \Omega_p$.
2. $u_\lambda(n) \equiv u_{\lambda_0}(n) (\text{mod } p^2)$ *for all* $n = 0, 1, \ldots, p^k - 1$ *and all* $\beta \in \Omega_p$.
3. *There exist* $A, B \in \Omega_p$ *such that* $u_\lambda(p^k) \equiv A + B\beta (\text{mod } p^2)$ *for all* $\beta \in \Omega_p$.

Then we have, with the notation $\lambda = \lambda_0 + p^{2k}\beta,\ \beta \in \Omega_p$ that

1. *$u_\lambda(n) \in \Omega_p$ for all $n < p^{k+1}$ and all $\beta \in \Omega_p$.*
2. *For every $n < p^{k+1}$ there is a polynomial $t_n \in \Omega_p[z]$ of degree $\le n/p^k$ such that $u_\lambda(n) \equiv t_n(\beta)(\bmod\ p^2)$ for all $\beta \in \Omega_p$.*
3. *There is a polynomial $T \in \Omega_p[z]$ of degree $\le p$ such that $u_\lambda(p^{k+1}) - T(\beta)/p^2 \in \Omega_p$ for all $\beta \in \Omega_p$.*
4. *Let T be as in (3). Then, up to a constant factor we have $T(x) \equiv F^{\sigma^k}(A + Bx)(\bmod\ p)$, where F is the characteristic polynomial of the eigenvalue problem $Lu \equiv \lambda u(\bmod\ p)$.*

Proof. Statement (1) is a direct consequence of Proposition 2 part (2). To prove statement (2) we invoke the recursion (10). Since $p^{2k}/n(s+t+1)$ is p-adically integral if $n < p^{k+1}$ the recursion

$$\gamma_n = \sum_{r+s+t=n-1} \frac{p^{2k}}{n(s+t+1)} b_r v_s \gamma_t (\bmod\ p)$$

has p-adically integral coefficients whenever $n < p^{k+1}$. Remember that the coefficients v_s come from the product $u_{\lambda,k}(z)(u_\lambda(p^k)z^{p^k-1} + u_\lambda(p^k-1)z^{p^k})$. Since $u_\lambda(p^k)$ equals a linear polynomial in β modulo p^2, we see that all v_s equal polynomials in β of degree at most 1 modulo p^2. Moreover, $v_s = 0$ if $s < p^k - 1$. This means that the indices t on the right hand side of the above recursion all satisfy $t \le n-1-(p^k-1) = n-p^k$. Using this recursion it is now a simple matter to show that the γ_n modulo p^2 are equal to polynomials in β of degree $\le n/p^k$ for all $n < p^{k+1}$. Assertion (2) then follows immediately after using $u(z) = u_k(z)g_k(z)$
To prove assertion (3) we look at recursion (10) for $n = p^{k+1}$ and consider it modulo Ω_p. Observe that the worst denominator that can occur is p^2 coming from the terms with $s + t + 1 = p^{k+1}$. Since all γ_t are polynomials of degree $\le t/p^k$ in β modulo p^2 and the v_s are at most linear in β mod p^2 and $v_s = 0$ when $s < p^k - 1$, it is now easy to see that $\gamma_{p^{k+1}}$ equals an expression of the form $\frac{T(\beta)}{p^2}$ modulo Ω_p where T is a polynomial of degree $\le p$. After using $u_\lambda(z) = u_{k,\lambda}(z)g_{k,\lambda}(z)$ we see that the same statement holds for $u_\lambda(p^{k+1})$, as asserted in part (3).
To prove assertion (4) we multiply (10) with $n = p^{k+1}$ by p and consider it modulo Ω_p. Note that all terms on the right hand side with $s+t+1 < p^{k+1}$ are in Ω_p. Of the terms with $s+t+1 = p^{k+1}$ the ones with p^k not dividing t are in Ω_p, because, by Proposition (2), $\gamma_t \equiv 0(\bmod\ p)$ for such t. Hence we are left with $t = (p-1)p^k, (p-2)p^k$ and $s = p^k - 1, 2p^k - 1$ respectively. Let us use the notation $G_m = \gamma_{mp^k}$ from Proposition 2. Then it follows that

$$\begin{aligned} pG_p \equiv \frac{T(\beta)}{p} &\equiv \frac{1}{p}(v_{p^k-1}G_{p-1} + v_{2p^k-1}G_{p-2})(\bmod\ \Omega_p) \\ &\equiv \frac{1}{p}(-(A + B\beta)G_{p-1} + G_{p-2})(\bmod\ \Omega_p) \end{aligned}$$

So, $T(\beta) \equiv -(A+B\beta)G_{p-1} + G_{p-2} (\text{mod } p)$. From the recurrence for G_m in Proposition 2 and the definition of the cahracteristic polynomial F in (6) we now infer that $T(\beta) = F^{\sigma^k}(A+B\beta)$. Hence assertion (4) follows. **qed**
Proof of Theorem 1. Proposition 1 tells us that if $|u_{p^k}|_p > 1$ for some $k \geq 0$ then $u(z)$ has radius of convergence strictly less than 1. In particular this means that $u(1) = -\lambda \in \Omega_p$. Moreover, $u_{p^k} \in \Omega_p$ for all $k \geq 0$. But then application of Proposition 2 part (2) implies that $u_n \in \Omega_p$ for all $n \geq 0$. **qed**

Proof of Theorem 3. We shall describe how to get successive approximations to any of the eigenvalues λ of (3). This should suffice to prove our Theorem.
Let us start by taking $\lambda \in \Omega_p$. Then $u_\lambda(n) \in \Omega_p$ for all $n < p$. Application of Proposition 3 parts (3),(4) with $k = 0$ tell us that there exists a p-th degree polynomial T such that $u_\lambda(p) - T(\lambda)/p^2 \in \Omega_p$ and $T(x) \equiv F(x)(\text{mod } p)$. By the non-degeneracy assumption F has p distinct roots in $\overline{\mathbb{F}}_p$. Hence they can be lifted to p distinct roots mod p^2 of $T(x)(\text{mod } p^2)$. Choose one of these roots, say λ_0. Then all choices λ in the residue class $\lambda_0(\text{mod } p^2)$ will make $u_\lambda(p)$ integral. Write $\lambda = \lambda_0 + p^2\beta$. Then

$$T(\lambda_0 + p^2\beta)/p^2 \equiv T(\lambda_0)/p^2 + T'(\lambda_0)\beta(\text{mod } p^2).$$

Putting $T(\lambda_0)/p^2 = A$ and $T'(\lambda_0) = B$ we see that the conditions of Proposition 3 are now satisfied for $k = 1$. Application of the Proposition tells us of the existence of another polynomial T satisfying $u_\lambda(p^2) - T(\beta)/p^2 \in \Omega_p$ for all $\beta \in \Omega_p$. We know that $T(x) \equiv F^\sigma(A+Bx)(\text{mod } p)$ and again get p values of β that make $u_\lambda(p^2)$ integral. Choose such a solution, call it λ_1 and replace β by $\lambda_1 + p^2\beta$. Now repeat the whole process to make $u_\lambda(p^3)$ integral.
We also see that, since we basically solve $F \equiv 0$ all the time, the numbers will lie in the same finite extension of $\mathbb{Q}_p(a)$. **qed**

Proof of Theorem 2. The factorisation of u mod p is a direct consequence of Proposition 2 part (1) as we let $k \to \infty$. The fact that the eigenvalue of f_{i_k} is $-u_{p^k}(\text{mod } p)$ follows from Proposition 2 part (2).
To show that any sequence $i_0, i_1, i_2, \ldots$ corresponds to a solution of $Lu = \lambda u$ we go back to the proof of Theorem 3. There, at every index p^k we had to choose a value of β such that $F^{\sigma^k}(A+B\beta) \equiv 0(\text{mod } p)$. By choosing β such that $A + B\beta = \lambda_{i_k}^{p^k}$ we can see to it that $u(z)$ factors with the prescribed sequence of factors $f_{i_0}, f_{i_1}, f_{i_2}, \ldots$. **qed**

Finally, in the introduction we promised to show that the only value $\lambda \in \mathbb{Z}$ for which the recurrence

$$(n+1)^2 u_{n+1} = (11n^2 + 11n - \lambda)u_n + n^2 u_{n-1}, \quad u_0 = 1, u_1 = -\lambda$$

has a solution in $\mathbb{Z}$ is the value $\lambda = -3$. Suppose we have a solution and let $u(z) \in \mathbb{Z}[[z]]$ be its generating function. We consider $u(z)$ modulo 3.

According to Theorem 2 there is a factorisation of the form

$$u(z) = f_{i_0}(z) f_{i_1}(z)^3 f_{i_2}(z)^9 \cdots (\mathrm{mod}\ 3)$$

where the $f_i(z)$ are the normalised polynomials of degree 2 which are eigenpolynomials to the eigenvalue equation (6). Since $u(z) \in \mathbb{Z}[[z]]$ the polynomials $f_{i_k}(z)$ should all be in $\mathbb{F}_3[z]$. However, the eigenvalue equation (6) in our case reads $\lambda(\lambda^2+1) \equiv 0 (\mathrm{mod}\ 3)$. So there is a unique eigenvalue in $\mathbb{F}_3$ and hence $f_{i_k}(z)$ is uniquely determined. This means that the sequence $i_0, i_1, i_2, \ldots$ is uniquely determined. This corresponds to a unique eigenvalue $\lambda \in \mathbb{Q}_3$ and thus, at most one eigenvalue in $\mathbb{Z}$.

F.Beukers
Department of mathematics
Utrecht University
P.O.Box 80.010
3508 TA Utrecht
Netherlands
email: beukers@math.uu.nl

References

1. Y.André, G-functions and Geometry, Aspects of Mathematics, Vieweg 1989
2. A.Adolphson, B.Dwork, S.Sperber, Growth of solutions of linear differential equations at a logarithmic singularity. Transactions AMS 271(1982), 245-252.
3. A.Beauville, Les familles stables de courbes elliptiques sur $\mathbb{P}^1$ admettant quatre fibres singulières, C.R.Acad. Sc.Paris 294 (1982), 657-660.
4. G.Christol, Systèmes différentiels linéaires p-adique, structure de Frobenius faible, Bull.Soc.Math. de France 109 (1981), 83-122.
5. D.V.Chudnovsky, G.V.Chudnovsky, Transcendental methods and Theta-functions, Proc. Symp. Pure Mathematics 49, part 2 (1989), 167-232.
6. B.Dwork, Differential operators with nilpotent p-curvature, Amer.J.Math. 112 (1990),749-786.
7. B.Dwork, Arithmetic theory of differential equations, Symp.Math. XXIV (INDAM, Rome), 225-243, Academic Press, 1981.
8. B.Dwork, Differential equations which come from geometry, Study group on ultrametric analysis 1982/83, exposée 9, Inst. Henri Poincar'e, Paris, 1984.
9. B.Dwork, G.Gerotto, F.J.Sullivan, An introduction to G-functions, Annals of Math. Studies 133, Princeton Univ. Press 1994.
10. D.R.Hofstadter, Energy levels and wave functions of Bloch electrons in rational and irrational magnetic fields, Phys.Rev 14 (1976), 2239-2249.
11. T.Honda, Algebraic differential equations, INDAM Symp. Math XXIV (1981), 169-204.
12. N.M.Katz, Algebraic solutions of differential equations, Inv. Math. 18(1972), 1-118.
13. B.Lian, S.T.Yau, Arithmetic properties of mirror maps and quantum coupling, Comm. Math. Phys. 176 (1996), 163-191.