Computational Problems in Arithmetic of Linear Differential Equations. Some Diophantine Applications

D.V. Chudnovsky, G.V. Chudnovsky*
Department of Mathematics
Columbia University
New York, New York 10027

INTRODUCTION. In diophantine approximation, particularly in effective methods of irrationality proving, a crucial role is played by sequences of integral (nearly integral) of rational or algebraic numbers satisfying finite order recurrences (with coefficients polynomial in indices). Generating functions of such sequences satisfy linear differential equations; and these generating functions belong to Siegel's class of G- functions [3]. In this presentation we examine G - function and linear differential equations that can have G - function solutions. We present a brief review of known results in this direction. Our new research is devoted mainly to the second order equations and three-term linear recurrences leading to classical Stieltjes' continued fraction expansions [50], [51]. A new instrument used in global and p-adic analysis of the linear differential equations is furnished by computational methods, including methods of computer algebra. Our numerical experiments, some of which are summarized in this presentation, show that linear differential equations satisfied by power series with nearly integral coefficients (G-function) possess special arithmetic properties that are associated with the existence of action of Frobenius. We present evidence for the conjecture that all such equations with G-function solutions arise from geometry, as Picard-Fuchs equations on variation of period (Hodge) structure of algebraic varieties. To study these, globally nilpotent equations, we use methods of diophantine approximations, particular Padé-type approximations.

To study linear differential equations p-adically, we examine "p-adic spectrum" of the Lamé equation. New examples of classes of globally nilpotent equations (of Lamé type) are constructed using Fuchsian arithmetic group (including quaternion groups). These equations are connected to diophantine equations to such numbers as $\varsigma(2), \varsigma(3)$ and periods of elliptic curves. Closely connected with these are new continued fraction expansions, presented below, generalizing Stieltjes-Rogers [49], [50], [51], [52], [53], [54] continued fraction expansions of integrals of elliptic functions. These new expansions are associated with Lamé equations with integral parameter n. We reexamine these equations, looking for those Lamé equations that have algebraic solutions only. The existence of such solutions is connected with zeros of special modular forms. We look,

*This work was supported in part by NSF grant DMS-8409626, Program O.C.R.E.A.E., U.S. Air Force (ACMP Program).

in particular, at Lamé equations over $\mathbf{Q}$, where the classification is, at least in principle, possible (and is achieved for small n).

Hypergeometric functions should, according to Siegel's conjecture [4] encompass the class of G-functions. Among these, special ${}_3F_2$ functions are associated with Ramanujan quadratic period relations [58], [48]. We present generalizations of these to other arithmetic triangle groups. We also build a new theory of p-adic "Ramanujan like" quadratic period relations that associate with every hypergeometric identity for an algebraic multiple of $1/\pi$ a series of modp^k congruences on partial sums of these series. Such congruences are naturally identifiable with action of Frobenius on linear differential equations on elliptic periods, specialized at curves with complex multiplication. Applications of these new congruences will be reported elsewhere.

Computational methods useful in theoretical study of elliptic curves, can also benefit from elliptic curve arithmetic. In the final part of this presentation we describe a class of fast interpolation algorithms generalizing FFT schemes. Such fast interpolation is particularly efficient in modular arithmetic on elliptic curves with highly composite Mordell-Weil group, because they can be used for an arbitrary prime p without any special binary structure.

We thank the Computer Algebra Group of IBM for their interest, help and access to their system SCRATCHPAD.

1 Globally Nilpotent Linear Differential Equations.

In this section we look at arithmetic properties of solutions of linear differential equations, that have solutions with special arithmetic properties. These special arithmetic properties are the near integrality properties of power series expansions of functions, known as G-functions.

A class of G-functions was introduced by Siegel in [3], a paper more famous for its diophantine equation treatment and classical results on a related class of E-functions.

Siegel's study of E-functions [3-4], were significantly advanced since then by many researchers, see particularly [5-6]. We would like to mention in this connection that only relatively recently we have proved results on the best possible measure of diophantine approximations of values of E- functions at rational points [7]. These results present an ultimate effective version of the Schmidt theorem [8] for the values of E - functions. The E - function $f(x)$ are entire functions with power series expansion $f(x) = \sum_{n=0}^{\infty} a_n x^n/n!$, where $a_n \in \overline{\mathbf{Q}}$ and for every $\epsilon > 0$, we have $|a_n| < (n!)^\epsilon$, denom$\{a_0, \ldots, a_n\} \leq (n!)^\epsilon : n \geq n_1(\epsilon)$. In algebraic geometry and analysis, however, most of the interesting functions are analytic only in the finite part of the complex plane and have better p-adic convergence properties; these are G-functions.

<u>Definition 1.1.</u> A function $f(x)$ with the expansion at $x = 0$:

$$f(x) = \sum_{n=0}^{\infty} a_n x^n$$

is called a G-function, if $f(x)$ satisfies a linear differential equation over $\overline{\mathbf{Q}}(x)$, if coefficients a_n are algebraic numbers, and if there is a constant $C > 1$ such that for all $n \geq 0$ the sizes of coefficients a_n (i.e. the maximum of absolute values of a_n and all its conjugates) and the common denominators den$\{a_0, \ldots, a_n\}$ are bounded by C^n.

Siegel in [3] only outlined a program of G-function values irrationality and transcendence results, similar to his E- function theorems. Progress in this direction became dependent on additional global conditions, requiring that the G-function property be satisfied by all other solutions of the same differential equation. Such a property a (G, C)-condition, first formulated in [9], we used to prove some G-functions results [9], [12], [11], [13].

In [14] and [15] we had proved the general linear independence results for values of arbitrary G-functions at algebraic points (close to the origin), without any additional conditions. These results materialize Siegel's program after some 55 years. We also have proved the strong (G, C)-property for arbitrary G- functions [20]. This result, connected with our study of the Grothendieck conjecture, implies, e.g. that all previous results on G-function theory, proved under very restrictive conditions, are unconditionally valid for all G-functions. To describe our result, and the (G, C)-function conditions, one needs the definition of the p-curvature.

We consider a system of matrix first order linear differential equations over $\mathbf{Q}(x)$, satisfied by functions $f_i(x) : i = 1, \ldots, n$:

$$df_i(x)/dx = \sum_{j=1}^{n} A_{i,j}(x) f_j(x), \tag{1.1}$$

for $A_{i,j}(x) \in \mathbf{Q}(x) : i, j = 1, \ldots n$. Rewriting the system (1.1) in the matrix form

$$df^t/dx = Af^t; A \in M_n(\mathbf{Q}(x)),$$

one can introduce the p-curvature operators Ψ_p, associated with the system (1.1) following [16], [17]. The p- curvature operators Ψ_p are defined for a prime p, as

$$\Psi_p = (d/dx - A)^p (\bmod p).$$

Then Ψ_p is a linear operator that can be represented as $\Psi_p = -A_p (\bmod p)$, where one defines for $m \geq 0$,

$$(d/dx)^m \equiv A_m (\bmod\, \mathbf{Q}(x)[d/dx](d/dx - A)). \tag{1.2}$$

Let $D(x)$ be a polynomial from $\mathbf{Z}[x]$ that is the denominator of A, i.e. $D(x)A_{i,j}(x)$ is a polynomial in $\mathbf{Z}[x]$ for $i, j = 1, \ldots, n$. The *(G,C)-function condition* [10]- [11] of (1.1) means that (1.1) is satisfied by a system $(f_1(x), \ldots, f_n(x))$ of G-functions, and that there exists a constant $C_2 > 1$, such that for any N, the common denominator of all coefficients of all polynomial entries of matrices $D(x)^m A_m(x)/m! : m = 0, \ldots, N$, is growing not faster than C_2^N. With this conditions is closely related a *global nilpotence* condition [15-18] stating that the matrices Ψ_p are nilpotent for almost all primes p. The (G, C)-condition implies the global nilpotence condition.

In [15] we proved the global nilpotence (and the (G, C)-function condition) of linear differential equations having a G-function solution. To prove this result we used Padé approximants of the second kind.

Theorem 1.2. Let $f_1(x), \ldots, f_n(x)$ be a system of G-functions, satisfying a system of first order linear differential equations (1.1) over $\overline{\mathbf{Q}}(x)$. If $f_1(x), \ldots f_n(x)$ are linearly independent over $\overline{\mathbf{Q}}(x)$, then the system (1.1) satisfies a (G, C)-function condition and is globally nilpotent. Any solution of (1.1) with algebraic coefficients in Taylor expansions is a G-function.

Padé approximation methods, used to prove the G-function Theorem 1.2, were also successfully applied by us to the study of the Grothendieck conjecture. The main tool in the study of the Grothendieck conjecture, and in the current study of globally nilpotent equations is the analytic method of Padé- (rational), and more general algebraic approximations to functions satisfying nontrivial complex analytic and arithmetic (p-adic) conditions. The corresponding group of results can be considered as a certain "local-global" principle. According to this principle, algebraicity of a function occurs whenever one has a near integrality of coefficients of power series expansion—*local conditions*, coupled with the assumptions of the analytic continuation (controlled growth) of an expanded function in the complex plane (or its Riemann surface)—a global, *archimedean* condition.

To prove the algebraicity of an integral expansion of an analytic function, assumptions on a uniformization of this function have to be made.

Our results from [19] and [20] were proved in the multidimensional case as well, to include the class of functions, uniformized by Jacobi's theta-functions (e.g. integrals of the third kind on an arbitrary Riemann surface). Moreover, our result includes "the nearly-integral" expansions, when the denominators grow slower than a typical factorial $n!$ denominator. In general, our results [19-20], show that $g+1$ functions in g variables having nearly integral power series expansions at $\overline{x} = \overline{0}$ and uniformized near $\overline{x} = \overline{0}$ by meromorphic functions of finite order of growth *are algebraically dependent*.

The first application of "local-global" principle was to the following:

The Grothendieck Conjecture. If a matrix system (1.1) of differential equations over $\overline{\mathbf{Q}}(x)$ has a zero p-curvature $\Psi_p = 0$ for almost all p, then this system (1.1) has algebraic function solutions only.

According to this conjecture, strong integrality properties of *all* power series expansions of solutions of a given linear differential equation imply that all these solutions are algebraic functions.

Methods of Padé approximations allowed us to solve the Grothendieck conjecture in important cases, [24], [15], [20] including the case of Lamé's equation, for integral n. In [25], it was shown that the Grothendieck conjecture is true for any linear differential equation all solutions of which can be parametrized by the meromorphic functions. The result was considerably generalized in [20] for equations, solutions of which can be parametrized by means of multidimensional theta-functions. To the class of these equations belong equations of rank one over arbitrary (finite) Riemann surfaces [20]:

Theorem 1.3 Any rank one linear differential equation over an algebraic curve, i.e. a first-order equation with algebraic function coefficients, satisfies the Grothendieck conjecture. Namely, if Γ is an algebraic curve (given by the equation $Q(z,w) = 0$) over

$\overline{\mathbf{Q}}$, and if the rank one equation

$$\frac{dF}{F} = \omega(z, w)dz \tag{1.3}$$

over $\overline{\mathbf{Q}}(\Gamma)$ (for an Abelian differential ωdz on Γ) is globally nilpotent, then all solutions of (1.3) are algebraic functions.

The relationship of the p-curvature operators with the monodromy (Galois) group of a differential equation is extremely interesting. Our methods, involving various generalizations of Padé approximations, allow us to prove the Grothendieck conjecture for a larger class of differential equations, when additional information on a monodromy group is available. A technique from [27] (cf. [28]) using a random walk method, allowed us to treat crucially important class of equations $Ly = 0$, whose monodromy group is up to a conjugation a subgroup of $GL_n(\overline{\mathbf{Q}})$.

While the Grothendieck conjecture describes equations, *all* solutions of which have nearly integral expansions, it is more important to find out which equations possess nearly integral or p-adically overconvergent (i.e. convergent in the p-adic unit disc, or, at least, better convergent than the p-adic exponent) solutions.

The p-adic overconvergence and the nearly integrality of solutions hold for linear differential equation with a natural action of Frobenius. A class of equations, where the action of Frobenius was studied by Dwork, Katz, Deligne and others is the class of Picard-Fuchs differential equations (for variation of periods or homologies of smooth and singular varieties), see reviews [1-2].

Next, all evidence points towards the conjecture that the globally nilpotent equations are only those equations that are reducible to Picard-Fuchs equations (i.e. equations satisfied by Abelian integrals and their periods depending on a parameter). As Dwork puts this conjecture, all globally nilpotent equations come from geometry.

Our results on G-functions allow us to represent this conjecture even in a more fascinating form. We call this conjecture Dwork-Siegel's conjecture for reasons to be explained later:

Dwork-Siegel Conjecture. Let $y(x) = \sum_{N=0}^{\infty} c_N x^N$ be a G-function (i.e. the sizes of c_N and the common denominators of $\{c_0, \ldots, c_N\}$ grow not faster than the geometric progression in N). If $y(x)$ satisfies a linear differential equation over $\overline{\mathbf{Q}}(x)$ of order n (but not of order $n-1$), then the corresponding equation is reducible to Picard-Fuchs equations. In this case $y(x)$ can be expressed in terms of multiple integrals of algebraic functions.

Siegel, in fact, put forward a conjecture which is, in a sense, stronger than the one given above. To formulate Siegel's conjecture we have to look again at his E-functions defined in [3]. Siegel showed that the class of E - functions is a ring closed under differentiation and integration. Siegel also studied the hypergeometric functions

$${}_mF_n\left({a_1,\ldots,a_m \atop b_1,\ldots,b_n}\middle|\lambda x\right)$$

for algebraic $\lambda \neq 0$, *rational* parameters $a_1, \ldots, a_m$ and $b_1, \ldots, b_n$ and $m \leq n$. These functions he called hypergeometric E=functions and suggested in [4] all E-functions can be constructed from hypergeometric E-functions.

Looking at the (inverse) Laplace transform of $f(x)$, we see that Siegel's conjecture translates into a conjecture on G-function structure stronger than Dwork-Siegel's conjecture given above. Indeed, it would seem that all Picard-Fuchs equations might be expressed in terms of generalized hypergeometric functions.

This stronger conjecture is not entirely without merit; e.g. one can reduce linear differential equations over $\overline{\mathbf{Q}}(x)$, satisfied by G-functions to higher order equations over $\overline{\mathbf{Q}}(x)$ with regular singularities at $x = 0, 1, \infty$ only–(like the generalized hypergeometric ones) cf. [27].

We are unable so far to give a positive answer to this Dwork-Siegel conjecture, that all arithmetically interesting ($G-$)functions are solutions of Picard-Fuchs equations. Nevertheless, in some cases we can prove that this conjecture is correct. For now our efforts are limited to the second order equations (which provides with an extremely rich class of functions).

Proposition 1.4 Let a second order equation over $\mathbf{Q}(x)$: $Ly = 0$ be a globally nilpotent one and it has zero p-curvature $\Psi_p = 0$ for primes p lying in the set of density $1/2$. Then the corresponding linear differential equation either have all of its solutions as algebraic functions, or is reducible to Picard-Fuchs equation (corresponding to the deformation of the curve), *or* has at least one transcendent element in a monodromy matrix for any representation of the monodromy group.

2 Arithmetic Properties and Diophantine Applications of Lamé Equations with n = -1/2.

Linear differential equations of the second order become arithmetically nontrivial when there is at least one accessory parameter. The first such case occurs for equations with 4 regular singularities. Among these a prominent role is played by the general Lamé equations; it is represented in the form [31-33]:

$$y'' + \frac{1}{2}\{\frac{1}{x} + \frac{1}{x-1} + \frac{1}{x-a}\}y' + \frac{B - n(n+1)x}{4x(x-1)(x-a)}y = 0 \tag{2.1}$$

depending on n and on accessory parameters B.

A more familiar form of the Lamé equation is the transcendental one, with the change of variables: $a = k^{-2}$, $x = (sn(u,k))^2$, [31]:

$$\frac{d^2y}{du^2} + k^2 \cdot \{B - n(n+1)sn^2(u,k)\}y = 0 \tag{2.2}$$

in terms of Jacobi sn-function. An alternative form of (2.1-2) is in terms of Weierstrass' elliptic function:

$$\frac{d^2y}{du^2} + \{H - n(n+1)\wp(u)\}y = 0. \tag{2.3}$$

Lamé equations are considered usually for integral values of the parameter n in (2.1-3). This is the only case when solutions of (2.3) (or (2.2)) are meromorphic functions in the u-plane. In the case of integral n the following facts are known [31,33]:

i) there exist $2n+1$ values of an accessory parameter (B in (2.2) or H in (2.3)) for which the algebraic form of the Lamé equation (2.1) has algebraic function solutions. These numbers $B_n^m : m = 1, \ldots, 2n+1$ are the ends of lacunas of the spectrum of an equation (2.2) considered as the spectral problem for the Lamé potential;

ii) all solutions of (2.2) and (2.3) are meromorphic functions of u of order of growth 2.

Moreover, for every $B \neq B_n^m$, two linearly independent solutions of (2.3) have the form

$$F_{\pm} = \Pi_{i=1}^{n} \frac{\sigma(a_i \pm u)}{\sigma(u)\sigma(a_i)} \cdot \exp\{\mp u \sum_{i=1}^{n} \varsigma(a_i)\}$$

for parameters a_i determined from B—all $\wp(a_i)$ are algebraic in terms of B.

If the Lamé equation (2.1) is defined over $\overline{\mathbf{Q}}$ (i.e. $a \in \overline{\mathbf{Q}}$ and $B \in \overline{\mathbf{Q}}$) our local-global principle of algebraicity can easily solve the Grothendieck conjecture for Lamé equations with integral n. We have proved in [25]:

<u>Theorem 2.1.</u> For integer $n \geq 0$ the Lamé equation has zero p-curvature for almost all p if and only if all its solutions are algebraic functions. The Lamé equation with integral n is globally nilpotent for $2n+1$ values of B: $B = B_n^m$—ends of lacunas of spectrum of (2.3).

For all other values of B, the global nilpotence of the Lamé equations with integral n over $\overline{\mathbf{Q}}$ is equivalent to the algebraicity of all solutions of (2.3).

The possibility of all algebraic solutions of (2.1) with $B \neq B_n^m$ was shown by Baldassari, and kindly communicated to us by Dwork. Such a possibility is discussed below.

For nonintegral n no simple uniformization of solutions of Lamé equation exits. Moreover, Lamé equations themselves provide the key to several interesting uniformization problems. An outstanding Lamé equation is that with $n = -1/2$. This equation (and some of its equivalents to be seen later) determine the uniformization of the punctured tori. This leads to the classical Poincaré-Klein [34-35] problem of accessory parameter, which in the case of (2.1) with $n = -1/2$ means the determination for any $a \neq 0, 1, \infty$ a unique value of B, for which the monodromy group of (2.1) is represented by real 2×2 matrices. This complex-analytic investigation of the complex analytic structure of the Lamé (and of the more general) equation and the accessory parameter had been actively pursued by Klein, Poincaré, Hilbert, Hilb [39], V. I. Smirnov [36], Bers [37] and Keen [38]. Recently accessory parameter problem was studied in connection with conformally invariant field theories by Polyakov, Takhtajan, Zograf and others, cf. [40].

The uniformization problem for the punctured tori case is particularly easy to formulate, and our efforts towards the examination of the arithmetic nature of Fuchsian groups uniformizing algebraic curves were initially focused on this case. The punctured tori case can be easily described in terms of Lamé equation with $n = -1/2$. If one starts with a tori corresponding to an elliptic curve $y^2 = P_3(x)$, then the function inverse to the automorphic function, uniformizing the tori arises from the ratio of two solutions of the Lamé equation with $n = -1/2$. If $P_3(x) = x(x-1)(x-a)$ (i.e. the singularities are at $x = 0$, 1, a and ∞), then the monodromy group of (2.1) is determined by 3 traces

$x = \mathrm{tr}(M_0M_1)$, $y = \mathrm{tr}(M_0M_a)$, $z = \mathrm{tr}(M_1M_a)$. Here M is a monodromy matrix in a fixed basis corresponding to a simple loop around the singularity a. These traces satisfy a single Fricke identity [38]:

$$x^2 + y^2 + z^2 - xyz = 0.$$

There exists a single value of the accessory parameter C for which the uniformization takes place. Equivalently, C is determined by conditions of reality of x, y, z.

Algebraicity Problem [32]. Let an elliptic curve be defined over $\overline{\mathbf{Q}}$ (i.e. $a \in \overline{\mathbf{Q}}$). Is it true that the corresponding (uniformizing) accessory parameter C is algebraic? Is the corresponding Fuchsian group a subgroup of $GL_2(\overline{\mathbf{Q}})$ (i.e. x, y and z are algebraic)?

Extensive multiprecision computations, we first reported in [32], of accessory parameters showed rather bleak prospect for algebraicity in the accessory parameter problems. Namely, as it emerged, there are only 4 (classes of isomorphisms of) elliptic curves defined over $\overline{\mathbf{Q}}$, for which the values of uniformizing accessory parameters are algebraic. These 4 classes of algebraic curves are displayed below in view of their arithmetic importance.

Why are we interested in algebraicity (rationality) of the accessory parameters?

It seems that attention to the arithmetic properties of the Lamé equation with $n = -1/2$ arose shortly after Apéry's proof of the irrationality of $\zeta(2)$ and $\zeta(3)$. His proof (1978), see [42], was soon translated into assertions of integrality of power series expansions of certain linear differential equations.

To look at these differential equations we will make use of the classical equivalence between the punctured tori problem and that of 4 punctures on the Riemann sphere. For differential equations this means Halphen's algebraic transformation from [31], [41] between the Lamé equation with $n = -1/2$:

$$P(x)y'' + \frac{1}{2}P'(x)y' + \frac{x + C}{16}y = 0, \tag{2.4}$$

for $P(x) = x(x-1)(x-a)$, and the Heun equation with zero-differences of exponents at all singularities:

$$P(x)y'' + P'(x)y' + (x + H)y = 0. \tag{2.5}$$

The relation between two accessory parameters is the following

$$C = 4H + (1 + a).$$

Let us denote the equation (2.5) by $Ly = 0$. We have already stated that there are 4 Lamé equations with $n = -1/2$ (up to Möbius transformations) for which the value of the accessory parameter is known explicitly and is algebraic. These are 4 cases when the Fricke equation

$$x^2 + y^2 + z^2 = xyz,$$

with $0 \le x \le y \le z \le xy/2$, has solutions, whose squares are integers. It is in these 4 cases, when the corresponding Fuchsian group uniformizing the punctured tori is the congruence (arithmetic) subgroup, see references in [32], [27].

Let us look at these 4 cases, writing down the corresponding equation (2.5):

1) $x(x^2-1)y''+(3x^2-1)y'+xy=0$.

2) $x(x^2+3x+3)y''+(3x^2+6x+3)y'+(x+1)y=0$.

3) $x(x-1)(x+8)y''+(3x^2-14x-8)y'+(x+2)y=0$.

4) $x(x^2+11x-1)y''+(3x^2+22x-1)y'+(x+3)y=0$.

Each of the equations 1)-4) is a pull-back of a hypergeometric function by a rational map, and, as a consequence, each of the equations is globally nilpotent. In fact, for each of the equations 1)-4) there exist an integral power series $y(x)=\sum_{N=0}^{\infty}c_N x^N$ satisfying $Ly=0$ and regular at $x=0$.

Apéry's example for $\varsigma(2)$ arises from the equation 4). In this case the solution $y(x)$ of 4), regular at $x=0$ has the form $y(x)\text{-}\sum_{N=0}^{\infty}c_N x^N$ with integral c_N. It is easy to see that a nonhomogeneous equation $Ly=\text{const}\neq 0$ has a solution $z(x)=\sum_{N=0}^{\infty}d_N x^N$ regular at $x=0$ with nearly integral d_N (this is according to the global nilpotence of the corresponding L).

The only (possible) singularities of $y(x)$ and $z(x)$ in the finite part of the plane are $x=(-11\pm 5\sqrt{5})/2$, where all local exponents are zero. Thus we can always find a constant ς such that $\varsigma\cdot y(x)+z(x)$ is regular at $x=\frac{-11+5\sqrt{5}}{2}=(\frac{\sqrt{5}-1}{2})^5$. Apéry determined theconstant ς; if one takes $z(x)=\sum_{N=0}^{\infty}d_N x^N$ as $Lz=5$, then $\varsigma=\varsigma(2)=\pi^2/6$.

One obtains the irrationality of $\varsigma(2)$, because c_N/d_N are dense approximations, and a nontrivial measure of irrationality of π^2 is derived too.

Other equations 1)-3) can be used in a similar way, because of their global nilpotence and existence of only 4 regular singularities. Apéry approximations to $\varsigma(3)$ arises from the equation 3), or rather from a symmetric square of the corresponding operator L.

These examples lead to a method of the construction of sequences of dense approximation to numbers using nearly integral solutions of globally nilpotent equations. Often the corresponding equations are Picard-Fuchs equations satisfied by generating functions of Padé approximants to solutions of special linear differential equations, see examples in [43], [44]. Apéry's approach is not the best for the purpose of improving measures of irrationality. But it gives a good starting point.

Diophantine approximations suggest the following problem: determine all cases of global nilpotence of Lamé equations.

Our intensive numerical experiments reveal a predictable, phenomenon: it seems that, with the exception of equations 1)-4) (and equations equivalent to them via Möbius transformations), there is *no* Lamé equations with $n=-1/2$ over $\overline{\mathbb{Q}}$ that are globally nilpotent. We put these observations as a

Conjecture 2.2. Lamé equations with $n=-1/2$ defined over $\overline{\mathbb{Q}}$ are not globally nilpotent except for 4 classes of equations corresponding to the congruence subgroups, with representatives of each class given by 1)-4).

What are our grounds for this conjecture? First of all, Padé approximation technique related to the Dwork-Siegel conjecture allows us to prove one positive result in the direction of this conjecture for the $n=-1/2$ case of the Lamé equation.

Theorem 2.3. For fixed $a \in \overline{\mathbf{Q}}$ ($a \neq 0,1$), there are only finitely many algebraic numbers C of bounded degree d such that the Lamé equation with $n = -1/2$ is globally nilpotent.

Similar results hold for any Lamé equation with rational n.

Of course, one wants a more specific answer for any n (e.g. for $n = -1/2$, there are only 4 classes of a and C given above with the global nilpotence). However for half-integral n, there are always $n + 1/2$ trivial cases of global nilpotence, where solutions are expressed in terms of elliptic integrals, see [31], [41].

We have started the study of globally nilpotent Lamé equations (2.4) or (2.5) with numerical experiments. This ultimately led to Conjecture 2.2.

We checked possible equations of the form (2.5) with

$$P(x) = x(x^2 - a_1 x + a),$$

i.e. 4 singularities at $x = 0, \infty$ and 2 other points, for values of

$$a_1, a \in \mathbf{Z}$$

in the box: $|a|, |a_1| \leq 200$. For all these equations (2.5) we checked their p-curvature for the first 500 primes. Our results clearly show that with an exception of 4 classes of equations equivalent to 1)-4), any other equation has a large proportion of primes p such that the p-curvature is not nilpotent for any $H \in \mathbf{Q}$!

An interesting p-adic problem arises when, instead of globally nilpotent equations one looks at the nilpotence conditions of p curvature for a fixed p or, equivalently, when thee is a p- integral solution for a fixed p. The only known case (Tate- Deligne) corresponds to Lamé equation with $n = 0$, where the unit root of the ς-function of the corresponding elliptic curve is expressed in terms of a unique accessory parameter. This example suggests a definition of p-adic spectrum, which we use only for Lamé equations.

We are interested in those H mod p for which the p-curvature of (2.6) is nilpotent, and particularly in those p- adic $H \in \mathbf{Z}_p$ for which there exists a solution $y = y(x)$ of (2.6) whose expansion has p-integral coefficients. We call those $H \in \mathbf{Z}_p$, for which such $y(x)$ exists, eigenvalues of (2.6) in the "p-adic domain", and their set we call "an integral p-adic spectrum". The problem of study of arithmetic nature of Lamé equation was proposed by I.M. Gelfand. Of course, if a p-curvature is not zero, there is no second solution $y(x)$ with the same property.

To determine p-adic spectrum we conducted intensive symbolic and numerical computations using SCRATCHPAD (IBM) and MACSYMA (Symbolics Inc.) systems.

We start with the observations of the "mod p" spectrum as p varies.

I. For noncongruence equations (2.5) with rational $a \neq 0,1$ (i.e. for an elliptic curve defined over $\mathbf{Q}$ with a point of order 2) there seem always to be infinitely many primes p for which *no* value of the accessory parameter H mod p gives a nilpotent p-curvature (thus mod p spectrum is empty).

Here are a few statistics for noncongruence equations with rational integers a:

For $a = 3$ the first p's with the null spectrum mod p are: $p =$ 61, 311, 677, 1699, 1783, 1811, 2579, 2659, 3253,... .

For $a = 5$ the first p's with the null spectrum mod p are: $p = 659$, 709, 1109, 1171, 1429, 2539, 2953, 2969, 3019, 3499, 3533, 3803, 3863, 4273, 4493, 4703, 4903, 5279, 5477, 5591, 6011, 7193, 7457, 7583,... .

For $a = 4$ the corresponding p's with the null spectrum are: $p = 101$, 823, 1583, 2003, 3499,... .

For $a = 13$ the corresponding list starts at: $p = 1451$, 1487, 2381,... .

Observation I above was checked by us for all noncongruent $P(x) = x(x^2 - a_1 x + a)$ with integral a_1, a not exceeding 250 in absolute value.

II. An integral p-adic spectrum of equations (7.2) with (p- integral) a has a complicated structure depending on the curve.

p-adic spectrum can be null, finite (typically a single element), or infinite, resembling the Cantor set.

Numerical analysis is not easy either. To study p-adic expansions of p-adic numbers from p-adic spectrum up to the order modp^k, one has to carry all the computations of rational functions and coefficients of power series expansions in the modular arithmetic modp^N for $N = 2(p^k - 1)/(p - 1)$. For example, in order to determine the 3-adic spectrum with 14 digits of precision (in the 3-adic expansion), one has to carry out computations with over 2,000,000 decimal digit long numbers! For congruence equations 1)-4) the p-adic spectrum seems to be an infinite one with a Cantor-like structure.

Like with the complex-analytic uniformization problem, there is a relationship with the p-adic uniformization of Mumford, particularly for curves with the multiplicative reduction at p.

3 Arithmetic of Lamé Equation for Different n.

Examples above show how globally nilpotent equations can be used for various irrationality and transcendence proofs. Picard- Fuchs equations, for example, provide generating functions for Padé approximants in Padé approximation problem to generalized hypergeometric functions, Pochhammer integrals and other classes of solutions of linear differential equations. We suggest, as a starting equation, when it is of the second order, an equation corresponding to an arithmetic Fuchsian subgroup. Congruence subgroups of $\Gamma(1)$ and quaternion groups provide with interesting families of globally nilpotent equations.

One can start with equations uniformizing punctured tori with more than one puncture. The complete description of arithmetic Fuchsian groups of signature $(1; e)$ had been provided by Maclachlan and Rosenberger [46] and Takeuchi [47]. These groups of signature $(1; e)$ are defined according to the following representation

$$\Gamma = < \alpha, \beta, \gamma | \alpha\beta\alpha^{-1}\beta^{-1}\gamma = -1_2, \gamma^e = -1_2 >,$$

where α and β are hyperbolic elements of $SL_2(\mathbf{R})$ and γ is an elliptic (respectively a parabolic) element such that $\mathrm{tr}(\gamma) = 2\cos(\pi/e)$.

For all $(1; e)$ arithmetic subgroups there exists a corresponding Lamé equation with a rational n, uniformized by the corresponding arithmetic subgroup. This way we obtain *73* Lamé equations, all defined over $\overline{\mathbf{Q}}$ (i.e. the corresponding elliptic curves and accessory parameter C are defined over $\overline{\mathbf{Q}}$). Some of these equations give rise to nearly integral sequences satisfying three-term linear recurrences with coefficients that are quadratic polynomials in n, and have the growth of their denominators and the convergence rate sufficient to provide the irrationality of numbers arising in this situation in a way similar to that of Apéry.

Groups of the signature $(1; e)$ correspond to the Lamé equations (see (2.1)):

$$P(x)y'' + \frac{1}{2}P'(x)y' + \{C - \frac{n(n+1)}{4}x\}y = 0$$

with $n + \frac{1}{2} = \frac{1}{2e}$.

In the arithmetic case one looks at totally real solutions of the modified Fricke's identity, which now takes the form:

$$x^2 + y^2 + z^2 - xyz = 2(1 - \cos(\frac{\pi}{e})).$$

Using numerical solution of the (inverse) uniformization problem, we determined the values of the accessory parameters. Among the interesting cases are the following:

Here $P(x) = x(x-1)(x-A)$ and:

(1;2)-case:

1) $A = 1/2$, $C = -3/128$,

$$(x = y = (1+\sqrt{2})^{\frac{1}{2}} \cdot 2^{\frac{3}{4}}, z = 2 + \sqrt{2});$$

2) $A = 1/4$, $C = -1/64$;
3) $A = 3/128$, $C = -13/2^{11}$;
4) $A = (2-\sqrt{5})^2$, $C = \sqrt{5} \cdot (2-\sqrt{5})/64$;
5) $A = (2-\sqrt{3})^4$, $C = -(2-\sqrt{3})^2/2^4$;
6) $A = (21\sqrt{33} - 27)/256$.

(1;3)-case

1) $A = 1/2$, $C = -1/36$
2) $A = 32/81$, $C = -31/2^4 \cdot 3^4$;
3) $A = 5/32$, $C = -67/2^9 \cdot 3^2$;
4) $A = 1/81$, $C = -1/2 \cdot 3^4$;
5) $A = (8 - 3\sqrt{7})/2^4$.

(1;4)-case

1) $A = -11 + 8\sqrt{2}$, C-cubic;
2. $A = (3 - \sqrt{8})/4$, C-cubic;

(1;5)-case

1) $A = 3/128$, $C = -397/2^{11} \cdot 5^2$;

In all cases above, A is real (as well as C) and $0 < A \leq 1/2$.

Not all elliptic curves corresponding to $(1; e)$-groups are defined over $\mathbf{Q}$—there is a nontrivial action of the Galois group (cf. with a different situation in [47]).

Let us return to the case of integral n, to complete the classification problem started in Theorem 2.1.

For linear differential equations, whose solutions are parametrized by meromorphic functions, our local-global algebraicity principle [19], [20], [25] proves the Grothendieck conjecture: if p-curvature is zero for almost all (density one) primes p, then all solutions of the equation are algebraic functions. A class of such linear differential equations includes equations known as "finite-band potentials" (familiar from the Korteweg-de Vries theory), among which the most prominent are Lamé equations with integer parameter n. These equations are parametrized by Baker's functions that are solutions of rank one equations over curves of positive genus, see [19]. For rank one equations the Grothendieck conjecture was proved in [19], see Theorem 1.3. According to this solution, if a rank one equation is globally nilpotent, its solutions are algebraic functions. Particularly simple and self contained proofs in the elliptic curve case can be found in §6 of [19] and in [25]. For Lamé equations our result implies that Lamé equations over $\overline{\mathbf{Q}}(x)$ with integral n can be globally nilpotent if and only if either the accessory parameter B is one of the lacunas ends B_n^m $(m = 1, \ldots, 2n+1)$, or else all solutions of Lamé equations are algebraic functions. In [25] we implicitly assume that Lamé equations over $\overline{\mathbf{Q}}(x)$ with integral n cannot have a finite monodromy group (all solutions are algebraic functions). In fact, Lamé equations for integral $n \geq 1$ with algebraic solutions only are possible. These exceptional equations correspond to nontrivial zeros of special modular forms, and are closely connected with interesting algebraicity problems for exponents of periods of incomplete elliptic integrals of the third kind. To understand these relationships we use Hermite's solution of Lamé equations [31]. Let us look at Weierstrass elliptic functions $\sigma(u), \zeta(u)$ and $\wp(u)$, associated with the lattice $L = 2\omega_1\mathbf{Z} + 2\omega_2\mathbf{Z}$ in $\mathbf{C}$. The Hermite's function is

$$H(v; u) = \frac{\sigma(u-v)}{\sigma(u)\sigma(v)} e^{\zeta(v)u}. \tag{3.1}$$

For $n = 1$ and $B = \wp(v)$ $(\neq B_1^m)$, two linearly independent solutions of Lamé equations are $H(\pm v; u)$. If $n \geq 1$ and $B \neq B_n^m$ $(m = 1, \ldots, 2n+1)$ then two linearly independent solutions of the Lamé equation with an integral n parameter can be expressed in the form

$$F = \sum_{j=0}^{n-1} b_j \frac{d^j}{du^j}\{H(v; u) \cdot e^{\rho u}\},$$

where $b_0, b_1, \ldots b_{n-1}, \rho, \wp(v)$ are determined algebraically over $\mathbf{Q}$ in terms of B and parameters g_2, g_3 of $\wp(x)$.

The monodromy group of Lamé equations with integral n can be thus easily expressed explicitly in terms of Floquet parameters. The general theory is outlined in [41] for arbitrary equations of "Picard type", where Floquet solutions in this, doubly periodic case, are called multiplicative solutions. Whenever the accessory parameter B is distinct from lacunas ends, the monodromy can be determined from the action of two translations $u \to u + 2\omega_1$ or $u \to u + 2\omega_2$ on Hermite's function $H(v, u)$. The rule of transformation of $H(v; u)$ is very simple: if $2\omega = 2m_1\omega_1 + 2m_2\omega_2$, then

$$H(v; u + 2\omega) = H(v; u) : \exp\{\varsigma(v)2\omega - v \cdot 2\eta\},$$

for $2\eta = 2m_1\eta_1 + 2m_2\eta_2$. Thus with every $H(v; u)$ function two Floquet parameters μ_1 and μ_2 are associated:

$$\mu_i = \exp\{\varsigma(v) \cdot 2\omega_i - v \cdot 2\eta_i\} : i = 1, 2. \tag{3.2}$$

Let us look at Floquet solutions of an arbitrary Lamé equation with integral n (or following notations of [41] at an arbitrary multiplicative solution of Picard equation). Such a solution can be expressed in the form

$$F(u) = H(v; u)e^{\rho u} \cdot P(u), \tag{3.3}$$

where $P(u)$ is an elliptic function of u. For such a solution to be algebraic in $\wp(u)$ it is necessary and sufficient for its Floquet parameters to be roots of unity. The Floquet parameters s_i of $F(u)$ defined as

$$F(u + 2\omega_i) = F(u) \cdot s_i : i = 1, 2,$$

are $s_i = \mu_i \cdot e^{\rho 2\omega_i} = \cancel{\exp\{\varsigma(v) \cdot v \cdot 2\eta_i + 2\rho\omega_i}\}$.

This gives two equations on v, solving which and taking into the account the Legendre identity $\eta_1\omega_2 - \eta_2\omega_1 = \frac{1}{2}\pi\sqrt{-1}$, we get

$$\varsigma(v) + \rho = -r_1 \cdot 2\eta_2 + r_2 \cdot 2\eta_1;$$

$$v = -r_1 \cdot 2\omega_2 + r_2 \cdot 2\omega_1,$$

if $s_i = \exp\{r_i \cdot 2\pi\sqrt{-1}\}$ for rational $r_i \in \mathbf{Q} : i = 1, 2$. This shows that $F(u)$ can be an algebraic function in $\wp(u)$ only if (but not necessarily) if v is a torsion point of L. The precise relations are presented above:

$$\begin{aligned} v &= \frac{n_1 \cdot 2\omega_1 + n_2 \cdot 2\omega_2}{N}; \\ \varsigma(v) + \rho &= \frac{n_1 \cdot 2\eta_1 + n_2 \cdot 2\eta_2}{N}, \end{aligned} \tag{3.4}$$

where $(n_1, n_2, N) = 1$. These relations express conditions on an elliptic curve (depending on N and the dependency of ρ on v) to have a solution $F(u)$ algebraic in $\wp(u)$ To express this relation in a more explicit form we use multiplication formula for elliptic functions. One of the best expression of multiplication formulas involves elliptic functions

$$\psi_N(u) \stackrel{def}{=} \frac{\sigma(Nu)}{\sigma(u)^{N^2}}$$

for $N \geq 1$. These elliptic functions satisfy the famous three-term (Weierstrass) non-linear recurrences, and some properties of these functions and their specializations are summarized in [74]. Using the $\psi_N(u)$-polynomials in $\mathcal{P}(u)$ and $\mathcal{P}'(u)$, we derive a multiplication formula for $\varsigma(u)$:

$$\varsigma(Nu) - N\varsigma(u) = \frac{1}{N}\frac{\frac{\partial}{\delta u}\psi_N(u)}{\psi_N(u)},$$

representing $\varsigma(Nu) - N\varsigma(u)$ as a rational function in $\mathcal{P}(u), \mathcal{P}'(u)$. This multiplication formula cannot, unfortunately be used directly for $u = v$ - the torsion point of order N exactly, if N is odd, because $\varsigma(u)$ has poles at lattice points. We can modify it, though, by considering $u = x + v$ at $x \to 0$ for N-th order torsion point v. This way we get for $v = (n_1 \cdot 2\omega_1 + n_2 \cdot 2\omega_2)/N$,

$$\{(n_1 \cdot 2\eta_1 + n_2 \cdot 2\eta_2)/N - N \cdot \varsigma(v)\} = \frac{1}{2N} \cdot \frac{\psi''_N(v)}{\psi'_N(v)}.$$

These multiplication laws allow us to express the conditions on $F(u)$ to be an algebraic function in $\mathcal{P}(u)$ in a concise form:

$$\begin{gathered} \psi_N(v) = 0 (\text{or } v \in \frac{1}{N}L \backslash L); \\ \rho = \frac{1}{2N} \cdot \frac{\psi''_N(v)}{\psi'_N(v)}. \end{gathered} \tag{3.5}$$

[The last expression always makes sense, because $\sigma(u)$ does not have multiple roots.]

This system of equations for a given N is actually a single condition on the parameter $\tau = \omega_1/\omega_2$ in H of the elliptic curve. Such conditions and explicit expressions of ρ and B in terms of $\mathcal{P}(v)$, allow us to find, for a given N and n, all the Lamé equations with integral parameter n that have algebraic solutions only (with the order of local monodromy group dividing N). For a given n this seems to give an infinite set of conditions (parametrized by N). In reality, at least for a fixed field of definition of the Lamé equation, the determination of all cases of algebraicity is easier. Let us look at those Lamé equations that are defined over $\mathbf{Q}(x)$, i.e. g_2, g_3 and B are rational numbers. We are looking at those torsion points v of order N that are defined over $\mathbf{Q}$ ($\mathcal{P}(v) \in \mathbf{Q}$). In view of Masur's theorem, N is bounded. This leaves us for any given n only with finitely many cases corresponding to $N = 2,3,4,5,6,7,8,9,10,12$. Nonobvious generalizations of this argument are possible for arbitrary algebraic number field K and Lamé equations defined over $K(x)$. Elliptic curves determined by such conditions have parameters τ that are nontrivial zeros of special modular forms of weights depending on n and N. For any given n and N such nontrivial zeros, and thus the invariants g_2 and g_3 of the corresponding elliptic curves, can be explicitly determined.

Let us take $n = 1$ in the Lamé equation (the case $n = 0$ is trivial—only $B = 0$ gives a globally nilpotent equation). For $n = 1$ and $B = \mathcal{P}(v)$ ($\neq B_1^m = e_m = \mathcal{P}(\omega_m)$), two linearly independent solutions of the Lamé equation are $H(\pm v; u)$, i.e. $\rho = 0$ in the expression for $F(u)$ above. Consequently, for $n = 1$ and a fixed N the equations defining the elliptic curve and v are:

$$\psi_N(v) = 0, \ \psi_N''(v) = 0. \tag{3.6}$$

This immediately shows that the case of even N is impossible. For odd $N \leq 9$ all solutions can be easily found using any computer algebra systems. We summarize these findings choosing for an elliptic curve simple notations:

$$y^2 = x^3 + ax + b,$$

i.e. $a = -g_2/4$, $b = -g_3/4$. For $N = 3$ the only solution of the equations above is

$$a = 0, \ b \neq 0 - \text{arbitrary}, \tag{3.7}$$

i.e. $y^2 = x^3 + 1$ is the only exceptional curve. For $N = 5$ one gets an equation on a, b:

$$2160b^2 - 6241a^3 = 0, \tag{3.8}$$

or $a = 2^2 \cdot 3 \cdot 5$, $b = 2 \cdot 5 \cdot 79$ is the solution with $a, b \in \mathbf{Z}$ and the corresponding torsion point x $(= \wp(v))$ is $x = -4$.

For $N = 7$ or $N = 9$ there is no rational solutions in a and b. For example, for $N = 7$ one gets the following equation on a and b that leads to a quadratic equation on the absolute invariant J:

$$-106709177088b^4 + 73256324400a^3b^2 + 137751312727a^6 = 0.$$

In short, there are only two Lamé equations with $n = 1$ over $\mathbf{Q}(x)$ having algebraic solutions only. They correspond to $N = 3$ and $N = 5$ and to two elliptic curves (3.6), (3.7) over $\mathbf{Q}$ given above.

The problem of algebraic solutions of Lamé equation has interesting transcendental translations. As we have seen, we are looking at Floquet parameters μ_i depending on v such that $\wp(v) \in \overline{\mathbf{Q}}$. One can ask a more general question: is μ_i algebraic (a root of unity)? As it was reported in [33], the transcendence theory shows that each $\mu_i = \exp\{\zeta(v) \cdot 2\omega_i - v \cdot 2\eta_i\}$ is *transcendental*, whenever v is not a torsion point, $\wp(v) \in \overline{\mathbf{Q}}$ and $g_2, g_3 \in \overline{\mathbf{Q}}$. Nothing had been known so far about torsion points v. To present a definitive result in this direction, we start with a reformulation of one case of Schneider-Lang theorem. If an elliptic curve, corresponding to $\wp$, $\wp$'s is defined over $\overline{\mathbf{Q}}$, if $\wp(v) \in \overline{\mathbf{Q}}$, $\rho \in \overline{\mathbf{Q}}$ and, as before in (3.3), $F(u) = H(v; u)e^{\rho u}$, then for a nonalgebraic $F(u)$, its Floquet parameter $F(u+\omega)/F(u)$ for $\omega \in L$, $\omega \neq 0$, is a transcendental number. On the other hand, if $F(u)$ is algebraic, then all its Floquet parameters are roots of unity (and thus algebraic). The classification problem for Lamé equations with algebraic solutions only is thus equivalent to the determination of all algebraic numbers of the form μ_i above. For elliptic curves over $\mathbf{Q}$ our results show that there are only two (up to isomorphism) elliptic curves with $\wp(v) \in \mathbf{Q}$ such that μ_i is algebraic (third and fifth roots of unity).

4 Arithmetic Continued Fractions.

The problem of explicit determination of all linear differential equations that have arithmetic sense (i.e. an overconvergence property or the existence of nontrivial solutions mod p) can be easily translated into a classical problem of nearly integral solutions to linear recurrences. This problem arose in works of Euler, Lambert, Lagrange, Hermite, Hurwitz, Stieltjes and others in connection with irrational continued fraction expansions of classical functions and constants.

Problem 4.1. Let u_n be a solution of a linear recurrence of rank r with coefficients that are rational (polynomial) in n:

$$u_{n+r} = \sum_{k=0}^{r-1} A_k(n) \cdot u_{n+k}$$

for $A_k(n) \in \overline{\mathbf{Q}}(n) : k = 0, \ldots, r-1$, and such that u_n are "nearly integral". Then the generating function of u_n is a function whose local expansion represents either an integral of an algebraic function or a period of an algebraic integral, i.e. a solution of Picard- Fuchs-like equation. The "near integrality" of u_n means that u_n are algebraic numbers whose sizes grow slower than factorials, i.e. for any $\epsilon > 0$, the sizes of u_n are bounded by $(n!)^\epsilon$, and whose common denominator also grows slower than a factorial: i.e. for any $\epsilon > 0$ the common denominator of $\{u_0, \ldots, u_n\}$ is bounded by $(n!)^\epsilon$.

For continued fractions this problem can be reformulated:

Problem$'$. Let us look at an explicit continued fraction expansion with partial fractions being rational functions of indices:

$$\alpha = [a_0; a_1, \ldots, A(n), A(n+1), \ldots],$$

for $A(n) \in \mathbf{Q}(n)$. Let us look then at the approximations P_n/Q_n to α defined by this continued fraction expansion:

$$\frac{P_n}{Q_n} = [a_0; a_1, \ldots, A(n-1), A(n)] :$$

$n \geq 1$, where $P_n, Q_n \in \mathbf{Z}$.

If the continued fraction representing α is convergent *and* for *some* $\epsilon > 0$

$$|\alpha - \frac{P_n}{Q_n}| < |Q_n|^{-1-\epsilon} :$$

$n \geq n0(\epsilon)$, i.e. if α is *irrational*, then the sequences P_n and Q_n of numerators and denominators in the approximations to α are arithmetically defined sequences; their generating functions represent solutions of Picard-Fuchs and generalized Picard-Fuchs equations.

The later equations correspond to deformations with possible irregular singularities, arising from Laplace and Borel transforms of solutions of ordinary Picard-Fuchs equations.

Remark. While partial fractions $a_n = A(n)$ are rational functions of n, the sequences P_n and Q_n are *not* rational or algebraic functions of n unless in very special cases, when α is reducible to a rational number.

One of the main purposes of our investigation was an attempt to establish, first empirically, that there are only finitely many classes of such continued fraction expansions all of which can be determined explicitly. One has to distinguish several types of numbers/functions α and Picard-Fuchs like equations that can occur when such a continued fraction expansion of α exists:

A. Θ-function parametrization. This is the case when a linear differential equation can be parametrized by Abelian or θ-functions. This is the case of linear differential equations reducible to the so-called finite band/isospectral deformation equations. In general, the continued fraction expansions representing appropriate α do not have an arithmetic sense. Here α depends on the spectral parameter (uniformizing parameter of the curve) and on the curve moduli. For special values of spectral parameter ("ends of lacunas"), α is represented as a convergent continued fraction expansion with an arithmetic sense. In this case we had completely determined all the cases of global nilpotence in our work on the Grothendieck conjecture, see [19]. We return to the class A of continued fractions in connection with Stieltjes-Rogers continued fraction expansions.

B. In this case the monodromy group of a linear differential equation associated with a linear recurrence of any rank is connected with one of triangle groups. These groups do not have to be arithmetic. The cases of finite Schwarz's groups and elliptic groups are easier to describe. The hyperbolic (Fuchsian) cases provide with a large class of equations of high rank that are the blowups of hypergeometric equations. This is the case of Apéry's recurrences and continued fractions. However, for any *given* rank r there are only *finitely many* linear differential equations that occur this way.

C. Not all arithmetic Fuchsian groups are directly related to triangle ones, though Jacquet-Langland correspondence suggests some relationship at least on the level of representations and underlying algebraic varieties in the SL_2 case. In any case, to class C belong those α's and continued fraction expansions for which the corresponding differential equation has an arithmetic monodromy group. Multidimensional arithmetic groups, particularly Picard groups and associated Pochhamer differential equations provide *classes* of continued (more precisely, multidimensional continued) fractions corresponding to periods on algebraic surfaces and varieties.

In applications to diophantine approximations, a particular attention is devoted to three-term linear recurrences like:

$$n^d \cdot u_n = P_d(n) \cdot u_{n-1} - Q_d(n) \cdot u_{n-2} : n \geq 2$$

for $d \geq 2$. Apart from trivial cases (reducible to generalized hypergeometric functions), our conjectures claim that for every $d \geq 1$, there are only finitely many classes of such recurrences and that they all correspond to deformations of algebraic varieties.

For $d = 2$ (second order equations) we have classified nontrivial three-term recurrences whose solutions are always nearly integral, assuming our integrality conjectures. Most of these recurrences are useless in arithmetic applications. There are a few new ones that give some nontrivial results. Among these recurrences are the following:

i) $2n^2u_n = 2(-15n^2+20n-7)\cdot u_{n-1} + (3n-4)^2\cdot u_{n-2}$;
ii) $3n^2u_n = (-12n^2+18n-7)\cdot u_{n-1} + (2n-3)^2\cdot u_{n-2}$;
iii) $n^2u_n = (-12n^2+18n-7)\cdot u_{n-1} + (2n-3)^2\cdot u_{n-2}$;
iv) $n^2\cdot u_n = (56n^2-70n+23)\cdot u_{n-1} - (4n-5)^2\cdot u_{n-2}$.
There is a larger class of rank $r > 2$ linear recurrences of the form

$$n^2\cdot u_n = \sum_{k=1}^{r} A_k(n)\cdot u_{n-k},$$

all solutions of which are nearly integral. Many of these recurrences (like iii) above) give rise to new irrationalities. E.g. we present the following new globally nilpotent equation ($r=3$):

$$4x(x^3+16x^2+77x-2)y'' + 8(2x^3+24x^2+77x-1)y' + (9x^2+70x+84)y = 0.$$

Recently, studying Lamé equations we discovered new classes of explicit continued fraction expansions of classical special functions related to arithmetic problems above. These continued fractions expansions generalize many Stieltjes-Roger's continued fraction expansions.

Stileltjes-Roger's expansions [50-54] include the examples:

$$\begin{gathered}\int_0^\infty sn(u,k^2)e^{-uz}du = \frac{1}{z^2+a-}\,\frac{1\cdot 2^2\cdot 3k^2}{z^2+3^2a-}\,\frac{3\cdot 4^2\cdot 5k^2}{z^2+5^2a-}\,\frac{5\cdot 6^2\cdot 7k^2}{z^2+7a^2-\dots}\\ z\int_0^\infty sn^2(u,k^2)e^{-uz}du = \frac{2}{z^2+2^2a-}\,\frac{2\cdot 3^2\cdot 4k^2}{z^2+4^2a-}\,\frac{4\cdot 5^2\cdot 6k^2}{z^2+6^2a-}\,\frac{6\cdot 7^2\cdot 8k^2}{z^2+8^2a-\dots}\end{gathered} \tag{4.1}$$

$a = k^2+1$.

In the case of expansion (4.1) the approximations P_m/Q_m to the integral in the left hand side of (4.1) are determined from a three-term linear recurrence satisfied by P_m and Q_m

$$(2m+1)(2m+2)\phi_{m+1}(z) = (z+(2m+1)^2a)\phi_m(z) - 2m(2m+1)k^2\phi_{m-1}(z).$$

Here $\phi_m = P_m$ or Q_m, and Q_m are orthogonal polynomials. The generating function of Q_n satisfy a Lamé equation in the algebraic form with a parameter $n=0$. Here z plays a role of the accessory or spectral parameter in the Lamé equation, and the corresponding solutions is

$$y(x) = \sum_{m=0}^{\infty} Q_m(z)\cdot x^m$$

the only solution regular at $x=0$. The generating function of P_m is a regular at $x=0$ solution of nonhomogeneous Lamé equation.

These special continued fraction expansions can be generalized to continued fraction expansions associated with any Lamé equation with an arbitrary parameter n.

For $n=0$ these closed form expressions represent the Stieltjes-Rogers expansions. For $n=1$ two classes of continued fractions from [32, §13] have arithmetic applications, because for three values of the accessory parameter H (corresponding to e_i-nontrivial

2nd order points) the Lamé equation is a globally nilpotent one and we have p-adic as well as archimedean convergence of continued fraction expansions. This way we obtain the irrationality and bounds on the measure of irrationality of some values of complete elliptic integrals of the third kind, expressed through traces of the Floquet matrices. Similarly, for an arbitrary integral $n \geq 1$, among continued fraction expansions, expressed as integrals of elliptic θ-functions, there are $2n+1$ cases of global nilpotence, when continued fractions have arithmetic sense and orthogonal polynomials have nearly integral coefficients.

Among new explicit continued fraction expansions is the expansion of the following function generalizing Stieltjes-Rogers:

$$\int_0^{\infty} \frac{\sigma(u-u_0)}{\sigma(u)\sigma(u_0)} e^{\zeta(u_0)u} du,$$

or

$$\int_{\omega}^{\omega+\omega'} \frac{\sigma(u-u_0)}{\sigma(u)\sigma(u_0)} e^{\zeta(u_0)u} du,$$

as a function of $x = \wp(u_0)$. In Jacobi's notations this function can be presented as

$$\int_0^{\infty} \frac{H(u+u_0)}{\Theta(u)} e^{-uZ(u_0)} du,$$

where Θ and H are Jacobi's notations for functions.

The three-term linear recurrence determining the J-fraction for the corresponding orthogonal polynomials has the following form:

$$Q_N(x) = Q_{N-1}(x) \cdot \{(l+k^2) \cdot (N-1)^2 + x\}$$
$$+Q_{N-2}(x) \cdot k^4 \cdot (N-1)^2 \cdot N \cdot (N-\frac{1}{2}) \cdot (N-\frac{3}{2}) \cdot (N-\frac{5}{2}).$$

Here $x = sn^2(u_0; k^2)$.

The more general J-fraction of the form

$$\ddots b_{n-1} + x - \cfrac{a_{n-1}}{b_n + x - \cfrac{a_n}{b_{n+1} + x - \ddots}},$$

with

$$a_n = k^4 \cdot n(n+1) \cdot (n+\frac{1}{2})(n-\frac{1}{2}) \cdot \{(n-1) \cdot (n-\frac{1}{2}) - \frac{m \cdot (m+1)}{4}\};$$
$$b_n = (1+k^2) \cdot (n-1)^2 : n \geq 2$$

is convergent to the integral of the form

$$\int_0^{\infty} \prod_{i=1}^{m} \frac{H(u-u_i)}{\Theta(u)\theta(u_i)} e^{-Z(u_i)u} du.$$

The generating function of the corresponding orthogonal polynomials is expressed in terms of solutions of a Lamé equation with parameter $m \geq 1$.

These continued fraction expansions might be the only new additions to cases, when both the function is explicitly known (as an integral of classical functions) and its continued fraction is known.

5 Archimedean and P-adic Quadratic Period Relations á la Ramanujan.

Let us turn to applications of arithmetic differential equations, combined with complex multiplication, to diophantine approximations.

As we had stated above, the only arithmetically interesting linear differential equations are globally nilpotent ones. As we have conjectured earlier, these equations are exactly Picard- Fuchs equations of deformation of period (Hodge) structure of algebraic varieties. The first nontrivial case is that of curves, and in this category, elliptic curves are the most widely studied. Deformation of periods of elliptic curves are described by linear differential equations, uniformized by classical congruence subgroups. The full $\Gamma(1)$ group leads to the modular invariant $J = J(\tau)$, and $\Gamma(2)$ to the invariant $\lambda = k^2(\tau)$.

To be more specific and more general, we remind the primitives from the uniformization theory. If Γ is an arithmetic group (an arithmetic Fuchsian subgroup of $SL_2(\mathbf{R})$, and $\phi = \phi(\tau)$ is the corresponding automorphic function of Γ on H, then the function inverse to $\phi(\tau = \tau(\phi))$, is represented as a ratio of two solutions of a second order linear differential equation

$$(\frac{d^2}{d\pi^2} + R(\pi))y = 0$$

with algebraic function coefficients over $\overline{\mathbf{Q}}(\pi)$.

If the genus of Γ is zero, the equation has rational function coefficients.

For triangle groups the corresponding linear differential equations are Gauss hypergeometric equations. For 4 triangle subgroups, commensurable with the full modular group, one arrives at 4 theories of hypergeometric function representation of periods of elliptic curves (corresponding to low level structures on these curves).

These 4 theories of hypergeometric function representations are all related by modular identities of a relatively simple form, such as a well known expression of $J(\tau)$ in terms of $\lambda(\tau)$:

$$J(\tau) = 2^8 \cdot \frac{(1 - \lambda + \lambda^2)^3}{\lambda^2 \cdot (1 - \lambda)^2}.$$

These and other few (from the whole garden of) modular identities are easily translated into the hypergeometric identities between the corresponding representation of periods.

In fact, they all are consequences of simple fractional transformations and a single quadratic relation valid for a large class of hypergeometric functions:

$$_2F_1(2a, 2b; c - a - b; z) = {}_2F_1(a, b; c - a - b; 4z(1 - z)).$$

This or another way such identities were picked up by Ramanujan, [58], see exposition in [48], who also looked at specializations of hypergeometric representation of periods and quasiperiod is of foliations of elliptic curves to curves with complex multiplication. At curves with complex multiplication, modular functions (and combinations of their derivatives) are known to take algebraic values. These algebraic expressions, plugged into hypergeometric functions, lead to hypergeometric function representations of Λ/Φ (and other numbers connected with logarithms of algebraic numbers) as values of (rapidly) convergent hypergeometric series. All necessary algebraic and complex multiplication statements can be found in Weil's book [59].

To introduce Ramanujan's series we first need Eisenstein's series:

$$E_k(\tau) = 1 - \frac{2k}{B_k} \cdot \sum_{n=1}^{\infty} \sigma_{k-1}(n) \cdot q^n$$

for $\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}$, and $q = e^{2\pi i \tau}$. In the $E_k(\tau)$ notations, the quasiperiod relation is expressed by means of the function

$$s_2(\tau) \stackrel{\text{def}}{=} \frac{E_4(\tau)}{E_6(\tau)} \cdot (E_2(\tau) - \frac{3}{\pi Im(\tau)}), \tag{5.1}$$

which is nonholomorphic but invariant under the action of $\Gamma(1)$.

Ramanujan proved that this function admits algebraic values whenever τ is imaginary quadratic. Moreover, Ramanujan transforms these relations into rapidly convergent generalized hypergeometric representation of simple algebraic multiples of $1/\pi$. To do this he used only modular functions and hypergeometric function identities. Let us start with Ramanujan's own favorite [58]:

$$\frac{9801}{2\sqrt{2}\pi} = \sum_{n=0}^{\infty} \{1103 + 26390n\} \frac{(4n)!}{n!^4 \cdot (4 \cdot 99)^{4n}}.$$

The reason for this representation of $1/\pi$ lies in the representation of $(K(k)/\pi)^2$ as a ${}_3F_2$-hypergeometric function. Apparently there are four classes of such representations [48] all of which were determined by Ramanujan: all based on four special cases of Clausen identity of a hypergeometric function (and all represented by Ramanujan):

$$F(a, b; a + b + \frac{1}{2}; z)^2 = {}_3F_2\left({2a, a+b, 2b \atop a+b+\frac{1}{2}, 2a+2b} \middle| z\right).$$

The Clausen identity gives the following ${}_3F_2$-representation for an algebraic multiple of $1/\pi$, following from (5.1):

$$\sum_{n=0}^{\infty} \{\frac{1}{6}(1 - s_2(\tau)) + n\} \cdot \frac{(6n)!}{(3n)! n!^3} \cdot \frac{1}{J(\tau)^n} \tag{5.2}$$

$$= \frac{(-J(\tau))^{1/2}}{\pi} \cdot \frac{1}{(d(1728 - J(\tau))^{1/2}}.$$

Here $\tau = (1 + \sqrt{-d})/2$. If $h(-d) = 1$, then the second factor in the right hand side is a rational number. The largest one class discriminant $-d = -163$ gives the most rapidly convergent series among those series where all numbers in the left side are *rational*:

$$\sum_{n=0}^{\infty} \{c_1 + n\} \cdot \frac{(6n)!}{(3n)! n!^3 (-640, 320)^n} = \frac{(640, 320)^{3/2}}{163 \cdot 8 \cdot 27 \cdot 7 \cdot 11 \cdot 19 \cdot 127} \cdot \frac{1}{\pi}.$$

Here

$$c_1 = \frac{13,591,409}{163 \cdot 2 \cdot 9 \cdot 7 \cdot 11 \cdot 19 \cdot 127}$$

and $J(\frac{1+\sqrt{-163}}{2}) = -(640,320)^3$.

Ramanujan provides instead of this a variety of other formulas connected mainly with the tree other triangle groups commensurable with $\Gamma(1)$. All four classes of ${}_3F_2$ hypergeometric functions (that are squares of ${}_2F_1$−representations of complete elliptic integrals via the Clausen identity). These are

$${}_3F_2\left({}^{1/2,1/6,5/6}_{1\quad ,1}|x\right) = \sum_{n=0}^{\infty} \frac{(6n)!}{(3n)!n!^3}\left(\frac{x}{12^3}\right)^n$$

$${}_3F_2\left({}^{1/4,3/4,1/2}_{1\quad ,1}|x\right) = \sum_{n=0}^{\infty} \frac{(4n)!}{n!^4}\left(\frac{x}{4^4}\right)^n$$

$${}_3F_2\left({}^{1/2,1/2,1/2}_{1\quad ,1}|x\right) = \sum_{n=0}^{\infty} \frac{(2n)!^3}{n!^6}\left(\frac{x}{2^6}\right)^n$$

$${}_3F_2\left({}^{1/3,2/3,1/2}_{1\quad 1}|x\right) = \sum_{n=0}^{\infty} \frac{(3n)!}{n!^3} \cdot \frac{(2n)!}{n!^2}\left(\frac{x}{3^3 \cdot 2^2}\right)^n.$$

Representations similar to (3.2) can be derived for any of these series for any singular moduli $\tau \in \mathbf{Q}(\sqrt{-d})$ and for any class number $h(-d)$, thus extending Ramanujan list [58] ad infinum.

Ramanujan's algebraic approximations to $1/\pi$ can be extended to the analysis of linear forms in logarithms arising from class number problems. All of them are natural consequences of Schwarz theory and the representation of the function inverse to the automorphic one (say $J(\tau)$) as a ratio of two solutions of a hypergeometric equation. One such formula is

$$\pi i \cdot \tau = \ln(k^2) - \ln(16) + \frac{G(\frac{1}{2}, \frac{1}{2}; 1; k^2)}{F(\frac{1}{2}, -\frac{1}{2}; 1; k^2)},$$

and another is Fricke's

$$2\pi i \cdot \tau = \ln(J) + \frac{G(\frac{1}{12}, \frac{5}{12}; 1-; \frac{12^3}{J})}{F(\frac{1}{12}, \frac{5}{12}; 1; \frac{12^3}{J})}.$$

Here $G(a,b;c;x) = \sum_{n=0}^{\infty} \frac{(a)_n (b)_n}{(c)_n n!} \cdot \{\sum_{j=0}^{n-1} (\frac{1}{a+j} + \frac{1}{b+j} - \frac{2}{c+j})\}$ is the hypergeometric function (of the second kind) in the exceptional case, when there are logarithmic terms. Similar theory can be constructed for all arithmetic triangle groups [48]. The basic object here is the automorphic function $\phi(\tau)$ for the arithmetic group Γ normalized by its values at vertices.

An analog of $s_2(\tau)$ that is a nonholomorphic automorphic form for Γ is

$$\frac{1}{\phi'(\tau)} \cdot \left\{\frac{\phi''(\tau)}{\phi'(\tau)} - \frac{i}{Im(\tau)}\right\}.$$

For $\phi(\tau) = J(\tau)$ one gets $s_2(\tau)$.

For example, let us look at a quaternion triangle group (0;3;22,6,6). In this case, instead of elliptic Schwarz formula one has the following representation of the normalized automorphic function $\phi = \phi(\tau)$ in H in terms of hypergeometric functions:

$$\frac{\tau + i(\sqrt{2}+\sqrt{3})}{\tau - i(\sqrt{2}+\sqrt{3})} = -\frac{3^{1/2}}{2^2 \cdot 2^{1/6}} \cdot \{\frac{\Gamma(1/3)}{\sqrt{\pi}}\}^6 \cdot \frac{F(\frac{1}{12}, \frac{1}{4}; \frac{5}{6}; \phi)}{\phi^{1/6} \cdot f(\frac{1}{4}, \frac{5}{12}; \frac{7}{6}; \phi)}.$$

Thus the role of π in Ramanujan's period relations is occupied in $(0,3;2,6,6)-$case by the transcendence $\{\frac{\Gamma(1/3)}{\pi}\}^6$.

In the case $0,3;2,4,6)-$group the representation of $\phi = \phi(\tau)$ is

$$\frac{(\sqrt{3}-1)\tau - i\sqrt{2}}{(\sqrt{3}-1)\tau + i\sqrt{2}} = -2(\sqrt{3}-\sqrt{2})\frac{\Gamma(\frac{1}{24})\Gamma(-\frac{5}{24})}{\Gamma(-\frac{13}{24})\Gamma(-\frac{17}{24})} \cdot \phi^{1/2} \cdot \frac{F(\frac{13}{24}, \frac{17}{24}; \frac{3}{2}; \phi)}{F(\frac{1}{24}, \frac{5}{24}; \frac{1}{2}; \phi)}.$$

This leads to a new transcendence:

$$\frac{\Gamma(\frac{1}{24})^4}{\{\Gamma(\frac{1}{3})\Gamma(\frac{1}{4})\}^2}.$$

Thus, generalizations of Ramanujan identities allows us to express constants, such as π and other $\Gamma-$factors, as values of rapidly convergent series with nearly integral coefficients in a variety of ways, with convergence improving as the discriminant of the corresponding singular moduli increases.

Rapidly convergent ${}_2F_1$ and ${}_3F_1$ representations of multiples of $1/\pi$ and other logarithms can be and are used for diophantine approximations to corresponding constants in the manner described for globally nilpotent equations. For this one constructs, starting from hypergeometric functions themselves, hypergeometric representation of Padé approximations to them. This specialization of these approximations to complex multiplication points give nearly integral sequences of numerators and denominators in the dense approximations to corresponding constants. Such dense sequences of approximations are used to determine the measure of irrationality (or to prove irrationality) of classical constants. We were conducting extensive computations in this direction, particularly for π, $\pi/\sqrt{3}$ and $\pi/\sqrt{2}$, and an interesting phenomenon was discovered. Apparently there is a large cancellation (common factors) between numerators and denominators in the sequences of dense approximations, as defined by the corresponding linear recurrences. Also we found some interesting congruences for these dense approximations that allow us to improve measures of irrationalities obtained using these sequences. These congruences have a definitive analytic p-adic sense.

Indeed, in addition to archimedean period relations in the complex multiplication case there are corresponding nonarchimedean ($p-$adic) relations reflecting the same modular numbers. These p-adic evaluations indicate the possibility of existence of p-adic interpretation of hypergeometric identities. Several attempts to give such interpretation were undertaken. One of the more successful is the Koblitz-Gross formula [73] giving p-adic interpretation of Gauss sums for Fermat curves in terms of Morita's p-adic Γ - and B - functions formulas as $p-$adic analogs of Selberg-Chowla formula for periods of elliptic curves with complex multiplication.

In our applications to congruences satisfied by hypergeometric approximations to multiples of $1/\pi$, we do not need a $p-$adic values of the full series, but rather congruences satisfied by truncated hypergeometric series that can be directly interpreted through Hasse invariants and traces of Frobenius.

We briefly describe the background of congruences, taking as our initial model the Legendre form of elliptic curves (and of their periods).

Elliptic curves in the Legendre form are given by the following cubic equation:

$$y^2 = x \cdot (x-1) \cdot (x-\lambda). \tag{5.3}$$

Legendre notations for periods of this curve (= complete integrals of the first kind) and quasiperiods (= complete integrals of the second kind) are, correspondingly,

$$K(\lambda), K'(\lambda)$$

and

$$E(\lambda), E'(\lambda),$$

where

$$K(\lambda) \stackrel{\text{def}}{=} \frac{\pi}{2} \cdot {}_2F_1(\frac{1}{2}, \frac{1}{2}; 1; \lambda),$$
$$E(\lambda) \stackrel{\text{def}}{=} \frac{\pi}{2} \cdot {}_2F_1(-\frac{1}{2}, \frac{1}{2}; 1; \lambda).$$

Similarly:

$$K'(\lambda) = K(\lambda'),$$
$$E'(\lambda) = E(\lambda')$$

for $\lambda + \lambda' = 1$.

We denote

$$K_\lambda = \frac{d}{d\lambda} K(\lambda),\ K'(\lambda),\ \text{etc.}$$

The classical Legendre identity

$$K \cdot E' + K' \cdot E - K \cdot K' \equiv \frac{\pi}{2},$$

is equivalent to a simple Wronskian relation for the hypergeometric equation corresponding to the function

$$F(\lambda) \stackrel{\text{def}}{=} {}_2F_1(\frac{1}{2}, \frac{1}{2}; 1; \lambda) = \sum_{n=0}^{\infty} \binom{2n}{n}^2 (\frac{\lambda}{2^4})^n. \tag{5.4}$$

This Wronskian relation is

$$F \cdot F'_\lambda + F' \cdot F^\lambda = \frac{1}{\lambda \cdot \lambda' \cdot \pi} \tag{5.5}$$

(or $K \cdot K'_\lambda + K' \cdot K_\lambda = \frac{1}{2 \cdot \lambda \cdot \lambda'} \cdot \frac{\pi}{2}$).

Over finite fields, there is a well known relation between Hasse invariants and mod p reduction of solutions of the (Picard - Fuchs = Legendre) period linear differential equation. Such a relationship is very general, and we recommend Clemen's book [70] or original Manin's papers [71-72] where such relations are derived via Serre's duality. For elliptic curve in the Legendre form mod p interpretation is particularly easy to express in terms of Legendre function $F(\lambda)$. If one looks at hypergeometric equation satisfied by $F(\lambda)$:

$$\lambda(1-\lambda)\frac{d^2y}{d\lambda^2}+(1-2\lambda)\frac{dy}{d\lambda}+\frac{1}{4}y=0,$$

then this equation is globally nilpotent mod p (as Picard-Fuchs), but does not have two solutions defined mod p. Thus, there is a preferred (unique) solution mod p. To obtain this polynomials solution one has to reduce all coefficients of the power series expansion of $F(\lambda)$ mod p, and then delete all coefficients that follow two consecutive zeroes. This way one arrives to a polynomials mod p, known as Hasse-Deuring polynomial:

$$H_p(\lambda)=\sum_{i=0}^{m}\binom{m}{i}^2\lambda^i,\ m\stackrel{\text{def}}{=}\frac{p-1}{2} \tag{5.6}$$

of degree $m=\frac{p-1}{2}$ in λ.

This polynomial carries mod p properties of the original elliptic curve (5.1):

<u>Lemma 5.1.</u> The trace $a_p(\lambda)$ of Frobenius of an elliptic curve (5.1) over $\mathbf{F}_p$ for $\lambda\in\mathbf{F}_p$ satisfies the following congruence:

$$a_p(\lambda)\equiv(-1)^m\cdot H_p(\lambda)\bmod p.$$

The number $N_p(\lambda)$ of $\mathbf{F}_p$- rational points on an elliptic curve (5.1) is

$$N_p(\lambda)\equiv 1-(-1)^m\cdot H_p(\lambda)\bmod p.$$

The relationship between $H_p(\lambda)$ (this time a polynomial, not a number) is summarized in the following Tate result.

<u>Lemma 5.2.</u> In the ring of formal power series $\mathbf{F}_p[[\lambda]]$ one has the following decomposition:

$$F(\lambda)=H_p(\lambda)\cdot H_p(\lambda^p)\cdot H_p(\lambda^{p^2})\dots. \tag{5.7}$$

This identity has, in fact, a full p-adic meaning, better represented in the form

$$\frac{F(\lambda)}{F(\lambda^p)}\equiv(-1)^m\cdot a_p(\lambda)$$

closely connected with the problem of canonical lifting of Frobenius and analytic continuation inside the supersingular disks in the $\lambda-$ plane.

The polynomial $H_p(\lambda)$ is a transformation of a Legendre polynomial $P_m(x)$ formally identified as follows:

$$H_p(\lambda)=(\lambda-1)^{-m}\cdot P_m\left(\frac{\lambda+1}{\lambda-1}\right):m=\frac{p-1}{2}.$$

Of course, analogs of Hasse-Dewing polynomials exist for all other models of elliptic curves (e.g. the $J-$ representation of these polynomials was studied by Igusa). All these representations can be transformed one into another by birational correspondences reflected in hypergeometric function identities and congruences.

A variety of congruences on Legendre polynomials (most notably Schur congruences and their generalizations to higher powers of primes, studied by us) are all related to the formal completions of elliptic curves.

A richer variety of congruences occur for values of Legendre polynomials corresponding to specific elliptic curves. These congruences again arise from formal groups of these elliptic curves, but are now directly expressed in terms of traces of Frobenius. For higher and composite radices such congruences are known Aitken-Swinnerton-Dyer congruences.

We pay special attention to curves (5.1) with complex multiplication (i.e. when λ is a singular moduli). In this case when the curve E has complex multiplication in the imaginary quadratic field K, the trace of Frobenius, or the value $H_p(\lambda$ of Hasse-Deuring polynomial has a variety of arithmetic interpretations. It is easier to look at one-class fields K. The half of the primes p are supersingular for the elliptic curve (5.1), i.e.

$$H_p(\lambda) \equiv 0 \bmod p.$$

These are the primes p that stay prime in K. For other good primes p, split in K, the trace of Frobenius or $H_p(\lambda)$ is explicitly determined from the representation $4p = a^2 + Db^2$, for discriminant D of K.

In fact, a variety of algorithms (starting from Jacobi and investigated by Eisenstein and others) use, as a solution to the problem of representing a prime as a binary quadratic form (typically a sum of two squares for $K =$ Gaussian field) expressions for $H_p(\lambda)$.

As a mod p counterpart to Γ-function representation of periods of elliptic curves with complex multiplication, one can mention similar binomial function (Morita's p-adic B-function) representation of values of $H_p(\lambda)$ at complex multiplication points due to Koblitz-Gross.

We look now at the simplest case of $\lambda = 1/2$. In this case we have

$$H_p(\frac{1}{2}) \equiv 2^m \cdot (-1)^k \binom{2k}{k} \bmod p \tag{5.8}$$

for $m = \frac{p-1}{2}$ and $k = \frac{p-1}{4}$.

The expression (5.8) holds in nonsupersingular case $p = 4k+1$. In the supersingular case $p \equiv 3 (\bmod 4)$,

$$H_p(\tfrac{1}{2}) \equiv 0 \bmod p. \tag{5.8$'$}$$

To have a full mod p analog of Legendre differential equations we also need an interpretation of

$$\frac{d}{d\lambda} H_p(\lambda)$$

at singular moduli λ. In the case $\lambda = 1/2$ simple Legendre polynomials identities show that

$$\frac{d}{d\lambda} H_p(\frac{1}{2}) \equiv 0 \bmod p \text{ for } p \equiv 1 \bmod 4, \tag{5.9}$$

and

$$\tfrac{d}{d\lambda}H_p(\tfrac{1}{2}) \equiv -2^{-m+1}\cdot(-1)^k\tbinom{2k}{k} \bmod p \tag{5.9'}$$

for $p = 4k+3$, $m = 2k+1$.

Comparing (5.8-8′), and (5.9-9′), we end up with the congruence

$$H_p(\lambda)\cdot\frac{d}{d\lambda}H_p(\lambda)|_{\lambda=1/2} \equiv 0 \bmod p \tag{5.10}$$

for all p (> 2).

This congruence is an immediate nonarchimedean counterpart of one of the three (reducible to a single one) original Legendre identities concerning complete integrals of the first and second kind at singular module. In terms of $F(\lambda)$ it is simply

$$F(\lambda)\cdot\frac{d}{d\lambda}F(\lambda)|_{\lambda=1/2} = \frac{2}{\pi}. \tag{5.11}$$

The congruences (5.8) represent congruences on truncated sums of hypergeometric series representing multiples of $1/\pi$ in this particular and all other Ramanujan-like identities.

Before we present these identities, we have to point to the appearance of a new number $\frac{d}{dx}H_p(\lambda)$ at a singular module λ. Unlike $H_p(\lambda)$, its derivative evaluated at singular moduli lacks immediate arithmetic interpretation. This invariant is associated not with the formal group of an elliptic curve itself, but with the (two dimensional) formal group of an extension of an elliptic curve by an additive group.

That object is parametrized by

$$(\wp(u), \wp'(u), \zeta(u) + z).$$

In the complex multiplication case, $\frac{d}{d\lambda}H_p(\lambda)$ is quite different in supersingular and nonsupersingular cases. In the nonsupersingular case, $\frac{d}{d\lambda}H_p(\lambda)$ can be expressed in terms of trace of Frobenius. In the supersingular case, however, an interpretation of $\frac{d}{d\lambda}H_p(\lambda)$ is more involved and requires a look at $p-$adic $L-$ functions of elliptic curves at (negative) integral points.

With each of the 4 theories of hypergeometric series representations of period relations we associate congruences for values of truncated series. Congruences differ depending on the order of truncation in an obvious sense, i.e. if a few consecutive coefficients in series are zero mod M, all higher coefficients are ignored mod M. This way one builds a "$p-$adic" interpretation of Ramanujan identities, without changing left hand side (though the full series are meaningless $p-$adically).

We start with the representative theory corresponding to the absolute invariant $J(\tau)$:

The "Ramanujan's identities" were

$$\sum_{n=0}^{\infty}\{c_1 + n\}\frac{(6n)!}{(3n)!n!^3}\frac{1}{J^n} = \frac{\delta_1}{\pi},$$

where

$$c_1 = \frac{1}{6}(1 - s_2(\tau)),$$

$$\delta_1 = \frac{1}{2}\sqrt{\frac{-J}{d(12^3 - J)}}$$

for $\tau = (1+\sqrt{-d})/2$, $J = J(\tau)$.

Now truncations of the ${}_3F_2-$ series in $\frac{1}{J}$ can be appropriately determined mod p. We put:

$$S_N^{(1)} \overset{\text{def}}{=} \sum_{n=0}^{N} \{c_1 + n\} \cdot \frac{(6n)!}{(3n)! \cdot n!^3} \cdot \frac{1}{J^n}.$$

<u>Theorem 5.3.</u> For all good primes p,

$$S_N^{(1)} \equiv 0 \bmod p$$

for $[p/6] \leq N < p$.

Let us look at other theories corresponding to congruence subgroups. To simplify notations we denote *all* theories as follows:

$$\sum_{n=0}^{\infty} \{c_1 + n\} \frac{(6n)!}{(3n)! n!^3} \cdot \frac{1}{J^n} = \frac{\delta_1}{\pi};$$

$$\sum_{n=0}^{\infty} \{c_2 + n\} \frac{(4n)!}{n!^4} \cdot \frac{1}{Y^n} = \frac{\delta_2}{\pi};$$

$$\sum_{n=0}^{\infty} \{c_3 + n\} \frac{(2n)!^3}{n!^6} \cdot \frac{1}{X^n} = \frac{\delta_3}{\pi};$$

$$\sum_{n=0}^{\infty} \{c^4 + n\} \cdot \frac{(3n)! \cdot (2n)!}{n!^5} \cdot \frac{1}{Z^n} = \frac{\delta_4}{\pi}.$$

In all these formulas J, Y, X, Z are singular moduli (complex multiplication) and constants c_1, δ_1, c_2, δ_2, c_3, δ_3, c_4, δ_4 lie in the corresponding Abelian extensions of field K of complex multiplication. They all are easily explicitly expressed in terms of Eisenstein's nonholomorphic series $s_2(\tau)$. More interestingly the choices of c_i, δ_i are *unique* anyway! This follows from our results on algebraic independence of periods and quasiperiods of elliptic curves with complex multiplication [68], [69].

[This last remark together with congruences and trivial bounds on degrees of c_i and δ_i gives another purely modular approach to determine c_i and δ_i as well as other values of nonholomorphic modular functions. In practice, such approach is quite efficient.]

In four theories above the singular moduli have the following expressions:

$$J = J(\tau);$$

$$Y = 2^6 \cdot (2\lambda/\lambda' + 1 + \lambda'/2\lambda)$$

for $\lambda = k^2(\tau)$, $\lambda + \lambda' = 1$;

$$X = 2^4/\lambda \cdot \lambda';$$

$$Z = 3^3/hh',$$

for $J = 3^3 \cdot (9-8h)^3/h^3h'$, $h+h'=1$.

For each of the theories we have congruences on truncated series:

Theorem 5.4. For any good prime p, and the corresponding singular moduli defined mod p, the truncated hypergeometric series satisfy the following congruences:

$$S^{(3)N} = \sum_{n=0}^{N} \{c_3 + n\} \cdot \frac{(2n)!^3}{n!^6} \cdot \frac{1}{X^n} \equiv 0 \bmod p^k,$$

for

$$[p^k/2] \leq N \bmod p^k < p^k$$

(i.e. replace $1/\pi$ by 0 mod p^k in the corresponding identity).

For two other theories we have, correspondingly:

$$S_N^{(2)} = \sum_{n=0}^{N} \{c_2 + n\} \cdot \frac{(4n)!}{n!^4} \cdot \frac{1}{Y^n} \equiv 0 \bmod p$$

for

$$[p/4] \leq N \bmod p < p;$$

$$S_N^{(4)} = \sum_{n=0}^{N} \{c_4 + n\} \cdot \frac{(3n)! \cdot (2n)!}{n!^5} \cdot \frac{1}{Z^n} \equiv 0 \bmod p$$

for

$$[p/3] \leq N \bmod p < p.$$

Similar congruences for these two theories, as well as for the previous one, hold with p replaced with p^k.

All these congruences are generalized to higher radix congruences by placing truncations at appropriate places. Moreover, there are additional congruences in the supersingular cases. For supersingular primes the truncated series of corresponding ${}_3F_2$ functions vanish mod p^2.

For example, let us look at one of Ramanujan's original series representing "pure rational approximation" to $1/\pi$:

$$\sum_{n=0}^{\infty} \binom{2n}{n}^3 \cdot \frac{42n+5}{2^{12n+4}} = \frac{1}{\pi}.$$

Let us look then at a truncated series:

$$\mathcal{F}_N(\lambda) \stackrel{\text{def}}{=} \sum_{n=0}^{N} \{\frac{(\frac{1}{2})_n}{n!}\}^3 \lambda^n.$$

Thus the identity above is

$$[42 \cdot \lambda \cdot \mathcal{F}'_\infty(\lambda) + 5 \cdot \mathcal{F}_\infty(\lambda)]|_{\lambda=1/64} = \frac{16}{\pi},$$

and corresponds to the complex multiplication by $\sqrt{-7}$.

For truncated series we have first the usual congruences:

$$[42 \cdot \lambda \cdot \mathcal{F}'_N(\lambda) + 5 \cdot \mathcal{F}_N(\lambda)]|_{\lambda=1/64} \equiv 0 \bmod p$$

for all

$$\frac{p-1}{2} \leq N < p.$$

Next, we have "supersingular congruences":

$$\mathcal{F}_N(\lambda)|_{\lambda=1/64} \equiv 0 \bmod p^2;$$

$$\mathcal{F}'_N(\lambda)|_{\lambda=1/64} \equiv 0 \bmod p$$

for $p \equiv 3, 5, 6 \bmod 7$.

6 Elliptic Interpolation Algorithms

We end this presentation with the description of new fast evaluation and interpolation methods on elliptic curves.

To describe our algorithms we look at a general rational function interpolation problem. In the partial fraction representation of rational functions one looks at the rational function with poles only at given (distinct) points: $\alpha_1, \ldots, \alpha_n$. The general form of such a rational function is

$$R(z) = \sum_{i=1}^{n} \frac{x_i}{z - \alpha_i}. \tag{6.1}$$

The evaluation problem for this function consists of simultaneous determination of n values of $R(z)$ at $z = \beta_1, \ldots, \beta_n$ (distinct from α_i):

$$y_j = R(z)\,|_{z=\beta_j} = \sum_{i=1}^{n} \frac{x_i}{\beta_j - \alpha_i} : j = 1, \ldots, n. \tag{6.2}$$

It is easy to see that the inverse to this transformation is the following explicit one:

$$x_i = -\sum_{j=1}^{n} \{\frac{P_B(\alpha_i)P_A(\beta_j)}{P'_A(\alpha_i)P'_B(\beta_j)}\} \frac{y_j}{\beta_j - \alpha_i} : \tag{6.3}$$

$i = 1, \ldots, n$. Here, $P_A(x), P_B(z)$ are polynomials of degree n having as roots $\{\alpha_i\}$, and $\{\beta_i\}$, respectively.

Into the scheme (6.1-3) fall discretizations of important one- and multi-dimensional integral transform (with a variety of quadrature approximations methods). Among singular integral transformations that can be described by direct and inverse schemes (6.2-3) the most obvious is the Hilbert transform on a circle. Its proper discretization, and computations via FFTs was described in detail by Henrici. A finite Hilbert transform corresponds in the scheme (6.2-3) to α_i being N-th roots of 1, and β_j being N-th roots of -1. Explicit expressions (after proper normalizations of x_i and y_i) of finite

Hilbert transform depends on N being odd or even. For N even finite Hilbert transform is the following:

$$\chi(2n+1) = \frac{2}{N} \sum_{2k \bmod N} f(2k) ctg \frac{\pi}{N}((2n+1) - 2k),$$

$$\chi(2n) = \frac{2}{N} \sum_{2k+1 \bmod N} f(2k+1) ctg \frac{\pi}{N}(2n - (2k+1))$$

for a direct transform, and reversing the order,

$$f(2n+1) = \frac{2}{N} \sum_{2k \bmod N} \chi(2k) ctg \frac{\pi}{N}((2n+1) - 2k),$$

$$f(2n) = \frac{2}{N} \sum_{2k+1 \bmod N} \chi(2k+1) ctg \frac{\pi}{N}(2n - (2k+1))$$

for inverse transform.

Henrici [75] described the reduction of Hilbert transform on an interval to the finite Hilbert transform. This reduction allows for computation of all integrals of the form

$$\frac{1}{\pi}\int_{-1}^{1} \frac{X(t)dt}{t-s} \text{ and } \frac{1}{\pi}\int_{-1}^{1} \frac{X(t)dt}{(1-t^2)(t-s)}.$$

The finite versions of these transforms correspond to schemes (6.2-3) with α_i and β_j being roots of Chebicheff polynomials of the first and second kind respectively. In these cases the computational cost of the corresponding finite transforms on a set of n points is $O(n \log n)$, because, as in FFT, any roots of unity are used. For general sets, of points α_i and β_j, the computational cost is $O(n \log^2 n)$, because one has to use general interpolation algorithms that are of much higher computations cost. In practice, these algorithms are not attractive unless for a very large n. In recent papers of Gerasoulis et. al, see [76], the problem of evaluation of rational functions is considered, and several $O(n \log^2 n)$ algorithms are proposed. In these papers, the problem of rational evaluation is referred to as "Trummer's problem" stated by Golub.

We present now several classes of fast rational evaluation algorithms with computational cost $O(n \log n)$, that generalize finite Hilbert transforms. These new transformations correspond to a variety of singular integrals taken over one- dimensional complex continuum and to singular integrals over fractal sets, and to singular integrals with elliptic function kernels. The latter transformations have interesting number theoretic and modular interpretation and we refer to them as Fast Elliptic Number Theoretic Transform (FENTT).

To describe transformations of this class that can be evaluated in $O(n \log n)$ operations, we look at α_i and β_j given as roots of polynomials $P_{\mathcal{A}}(z)$ and $P_{\mathcal{B}}(z)$, respectively, where polynomials $P_{\mathcal{A}}$ and $P_{\mathcal{B}}$ correspond to iteration of (fixed) polynomials and rational functions. Thus we start with a sequence of degrees (radices) $D_1, \ldots, D_m$ and with rational functions (polynomials) $R_1(z), \ldots, R_m(z)$ of degrees D_1

$, \ldots, D_m$, respectively. The polynomials P_A and P_B have degrees $n = D_1 \ldots D_m$ and have roots as preimages of two distinct points α and β under iterated mappings

$$z_{i+1} = R_i(z_i).$$

Thus $P_A(z)$ is defined as (the numerator of) $R_m(R_{m-1}(\ldots(R_1(z))\ldots)) = \alpha$, and $P_B(z)$ as (the numerator of) $R_m(R_{m-1}(\ldots(R_1(z))\ldots)) = \beta$.

The most interesting case is that of $D_1 = \ldots = D_m = D$ and $R_1 = \ldots\ R_m = R$ being a fixed rational function of degree D. The fast algorithm is similar in the flow diagram to the mixed radix FFT schemes. This is a standard divide and conquer scheme in which one replaces the computation of (6.2) with

$$\begin{aligned} P_A(z) &\sim R_m(R_{m-1}(\ldots)) = \alpha \\ P_B(z) &\sim R_m(R_{m-1}(\ldots)) = \beta \end{aligned} \tag{6.4}$$

to the computation of D transforms of the form (6.2) for D pairs:

$$\begin{aligned} P'_A(z) &\sim R_{m-1}(\ldots) = \alpha' \\ P'_B(z) &\sim R_{m-1}(\ldots) = \beta' \end{aligned} \tag{6.5}$$

The mixed radix FFT algorithm is a special case of (6.4-5) with $R_i(z) = z^{D_i}$: $i = 1, \ldots, m$. The total computational cost of such mixed degree algorithm depends on the computational cost of multiplication of polynomials of degrees $O(D_i)$. In case of $D_i = O(D)$, and of large m, the total computational cost of evaluation of (6.2) is $O(mD_1 \ldots D_m)$.

Among rational transforms that fit into this scheme we can mention: a) Hilbert-like transforms for various Julia sets corresponding to polynomial or rational mappings $z \to R(z)$; b) singular integral transformations with elliptic function kernels. In the case a), contours of integration can have arbitrary fractional dimension. In the case b), a continuous analog of the transformation (6.2) is the following:

$$Y(s) = \int_0^{\omega} X(t)\wp(t-s)dt$$

for the Weierstrass elliptic function $\wp(u)$. The latter transform and its discrete versions are particularly well-suited for arithmetic interpretations. If an elliptic curve $\mathbf{E}$ is defined over a finite field $k = \mathbf{F}_p$ (e.g. is a reduction mod p of an elliptic curve over $\mathbf{Q}$), then the set of its k-rational points is an Abelian group of order $N_p = p - a_p + 1$ for $|a_p| \leq 2\sqrt{p}$. Moreover, for any integral a, $|a| < 2\sqrt{p}$, there is an elliptic curve over $\mathbf{F}_p$ with $N_p = p - a + 1$. Whenever 2^n divides N_p, one has points of order 2^n on an elliptic curve, all defined over $\mathbf{F}_p$. Consequently, the fast evaluation algorithm (6.4-5) can be applied in this case with $D_1 = \ldots = D_m = 4$. The rational function $R(z)$ in this case is the duplication formula for x-coordinate in the Weierstrass cubic form of an elliptic curve $E : y^2 = 4x^3 - g_2x - g_3$:

$$R(x) = -2x + \frac{(6x^2 - g_2/2)^2}{4y^y}$$

In (6.4) the choice of α and β should be of x- coordinates of second order points on E. Whenever prime p is such that p is within distance $2\sqrt{p}$ from a power of 2 (or from a highly composite number) one has a very fast algorithm of rational evaluation and transformation of length $O(p)$ mod p.

The same method can be used for a composite number of M if one chooses an appropriate elliptic curve over $\mathbf{Z}/M\mathbf{Z}$, whose reduction mod p for prime factors p of M have highly composite Abelian group of $\mathbf{F}_p$-rational points. Using the standard facts of the distribution of highly composite numbers, see [74], we conclude that with any number M we have FENTT of length $O(M)$ over $\mathbf{Z}/M\mathbf{Z}$ with computational cost $O(M \log M)$. FENTT algorithms are particularly attractive in parallel implementation because they can be executed in parallel for many primes and many elliptic curves with a full result brought together via Chinese remainder theorem.

As an extra application of FENTT, one can use torsion divisors on elliptic curves to decrease the additive complexity of polynomial multiplication and convolution using FENTT.

REFERENCES

[1] P. Griffiths, Periods of integrals on algebraic manifolds: summary of main results and discussion of open problems, Bull. Amer. Math. Soc., 75 (1970), 228-296.

[2] N. Katz, Nilpotent connections and the monodromy theorem: applications of a result of Turrittin, Publ. Math. I.H.E.S., 32 (1970) 232-355.

[3] C.L. Siegel, Über einige Anwendungen diophantischer Approximationen, Abh. Preuss. Akad. Wiss. Phys. Math. Kl., 1, 1929.

[4] C.L. Siegel, Transcendental Numbers, Princeton University Press, Princeton, 1949.

[5] A.B. Shidlovsky, The arithmetic properties of the values of analytic functions, Trudy Math. Inst. Steklov, 132 (1973), 169- 202.

[6] A. Baker, Transcendental Number Theory, Cambridge University Press, Cambridge, 1975.

[7] G. V. Chudnovsky, On some applications of diophantine approximations, Proc. Nat'l. Acad. Sci. USA, 81 (1984), 1926- 1930.

[8] W. M. Schmidt, Diophantine Approximations, Lecture Notes Math., v. 785, Springer, N.Y. 1980.

[9] A.L. Galočhkin, Lower bounds of polynomials in the values of a certain class of analytic functions, Mat. Sb., 95 (1974), 396-417.

[10] G. V. Chudnovsky, Padé approximations and the Riemann monodromy problem, in Bifurcation Phenomena in Mathematical Physics and Related topics, D. Reidel, Boston, 1980, 448-510.

[11] G. V Chudnovsky, Measures of irrationality, transcendence and algebraic independence. Recent progress, in Journees Arithmetiques 1980 (Ed. by J.V. Armitage), Cambridge University Press, 1982, 11-82.

[12] E. Bombieri, On G-functions, in Recent Progress in Analytic Number Theory (Ed. by H. Halberstram and C. Hooly), Academic Press, N.Y., v. 2, 1981, 1-67.

[13] K. Väänänen, On linear forms of certain class of G-functions and p-adic G-functions, Acta Arith., 36 (1980), 273-295.

[14] G. V. Chudnovsky, On applications of diophantine approximations, Proc. Nat'l. Acad. Sci. USA, 81 (1984), 7261- 7265.

[15] D.V. Chudnovsky, G.V. Chudnovsky, Applications of Padé approximations to diophantine inequalities in values of G- functions, Lecture Notes Math., v. 1135, Springer, N.Y., 1985, 9- 51.

[16] N. Katz, Algebraic solutions of differential equations, Invent. Math., 18 (1972), 1-118.

[17] T. Honda, Algebraic differential equations, Symposia Mathematica, v. 24, Academic Press, N.Y., 1981, 169-204.

[18] B. Dwork, Arithmetic theory of differential equations, ibid., 225-243.

[19] D. V. Chudnovsky, G.V. Chudnovsky, Applications of Padé approximations to the Grothendieck conjecture on linear differential equations, Lecture Notes Math., v. 1135, Springer, N.Y. 1985, 52-100.

[20] D.V. Chudnovsky, G.V. Chudnovsky, Padé approximations and diophantine geometry, Proc. Nat'l. Acad. Sci. USA, 82 (1985), 2212-2216.

[21] J.-P. Serre, Quelques applications du théoreme de densité de Chebtarev, IHES Pulb. Math., 54 (1981), 323-401.

[22] G. Faltings, Eudichkeitssätze für abelsche varietäten über zahlkörpern, Invent. Math., 73 (1983), 349-366.

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

[24] D.V. Chudnovsky, G.V. Chudnovsky, p-adic properties of linear differential equations and Abelian integrals, IBM Research Report RC 10645, 7/26/84.

[25] D.V. Chudnovsky, G.V. Chudnovsky, The Grothendieck conjecture and Padé approximations, Proc. Japan Acad., 61A (1985), 87-90.

[26] N. Katz, A conjecture in the arithmetic theory of differential equations, Bull. Soc. Math. France, 110 (1982), 203-239; corr., 347-348.

[27] D. V. Chudnovsky, G.V. Chudnovsky, A random walk in higher arithmetic; Adv. Appl. Math., 7 (1986), 101-122.

[28] G.V. Chudnovsky, A new method for the investigation of arithmetic properties of analytic functions, Ann. Math., 109 (1979), 353-377.

[29] C. Matthews, Some arithmetic problems on automorphisms of algebraic varieties, in Number Theory Related to Fermat's Last Theorem, Birkhauser, 1982, 309-320.

[30] B. Dwork, P. Robba, Effective p-adic bounds for solutions of homogeneous linear differential equations, Trans. Amer. Math. Soc., 259 (1980), 559-577.

[31] E. Whittaker, G. Watson, Modern Analysis, Cambridge, 1927.

[32] D.V. Chudnovsky, G.V. Chudnovsky, Computer assisted number theory with applications, Lecture Notes. Math., v. 1240, Springer, N.Y. 1987, 1-68.

[33] D.V. Chudnovsky, G.V. Chudnovsky, Remark on the nature of the spectrum of Lamé equation. Problem from transcendence theory., Lett Nuovo Cimento, 29 (1980), 545-550.

[34] H. Poincaré, Sur les groupes les équations linéaires, Acta Math., 5 (1884), 240-278.

[35] R. Fricke, F. Klein, Vorlesungen über die theorie der Automorphen Functionen, bd. 1., Teubner, 1925.

[36] V. I. Smirunov, Sur les équations differentielles linéaires du second ordre et la théorie des fouctions automorphes, Bull. Soc. Math. 45 (2) (1921), 93-120, 126-135.

[37] L. Bers, Quasiconformal mappings, with applications to differential equations, function theory and topology, Bull. Amer. Math. Soc., 83 (1977), 1083-1100.

[38] L. Keen, H.E. Rauch, A.T. Vasques, Moduli of unctured tori and the accessory parameter of Lamé's equation, Trans. Amer. Math. Soc., 255 (1979), 201-229.

[39] E. Hilb, Lineare Differentialgleichungen im komplexen Gebiet, Enzyklopädie der Math. Wissenschaften II, Band 6, Teubner, 1917, 471-562.

[40] L. A. Takhtadjan, P.G. Zograf, The Liouville equation action—the generating function for accessory parameter, Funct. Anal., 19 (1975), 67-68.

[41] E. G. C. Poole, Introduction to the Theory of Linear Differential Equations, Oxford, 1936.

[42] A. J. Van der Poorten, A proof that Euler missed... Appery's proof of the irrationality $\varsigma(3)$. Math. Intelligencer, 1 (1978/79), 195-203.

[43] D.V. Chudnovsky, G.V. Chudnovsky, Padé and rational approximations to systems of functions and their arithmetic applications, Lecture Notes Math., v. 1052, Springer, N.Y., 1984, 37-84.

[44] D.V. Chudnovsky, G.V. Chudnovsky, The use of computer algebra for diophantine and differential equations, in Computer Algebra as a Tool for Research in Mathematics and Physics, Proceedings of the New York Conference 1984, M. Dekker, N.Y.(to appear).

[45] B. Dwork, A deformation theory for the zeta function of a hypersurface. Proc. Intern. Congr. Math. Stockholm, 1962, Djursholm, 1963, 247-259.

[46] C. Maclachlan, G. Rosenberg, Two-generator arithmetic Fuchsian groups, Math. Proc. Cambridge Phil. Soc., 93 (1983), 383-391.

[47] K. Takeuchi, Arithmetic Fuchsian groups with signature $(1; e)$ J. Math. Soc. Japan, 35 (1983), 381-407.

[48] D.V. Chudnovsky, G.V. Chudnovsky, Approximations and complex multiplication according to Ramanujan, in Proceedings of the Ramanujan Centenary Conference, Ed. by R. Berndt, Academic Press, (to appear), 97pp.

[49] R. Askey, Orthogonal polynomials and theta functions, Proc. of 1988 AMS Summer School on Theta - Functions (in print).

[50] T.J. Stieltjes, Sur la réduction en fraction continue d'une série procédant suivant les puissances descendantes d'une variable, Ann. Fac. Sci. Toulouse, 3 (1889), 1-17. $\equiv$ Oeuvres, t. II, Groningen, 1918, 184-200.

[51] T. J. Stieltjes, Recherches sur lest fractions continue, ibid, 8 (1894), 1-22; 9 (1895), 1-47 $\equiv$ Ouevres, t. II, Groningen, 1918, 402-566.

[52] L. J. Rogers, On the representation of certain asymptotic series as convergent continued fractions, Proc. London, Math. Soc., (2), 4 (1907), 72-89.

[53] I.J. Schur, Ueber Potenzreihen die im Invern des Einheitskreises beschränkt sind, J. Reing Angev. Math., 147 (1916), 205-232; 148 (1917), 122-145.

[54] L. Carlitz, Some orthogonal polynomials related to elliptic functions, Duke Math. J., 27 (1960), 443-460.

[55] G.V. Chudnovsky, The inverse scattering problem and its applications to arithmetic, algebra and transcendental numbers, Lecture Notes Physics, v. 120, Springer, N.Y., 1980, 150-198.

[56] G.V. Chudnovsky, Rational and Padé approximations to solutions of linear differential equations and the monodromy theory, in Proceedings of the Les Houches International Colloquium on Complex Analysis and Relativistic Quantum Field Theory, Lecture Notes Physics, c. 126, Springer, N.Y., 1980, 136- 169.

[57] G.V. Chudnovsky, Number theoretical applications of polynomials with rational coefficients defined by extremality conditions, in Arithmetic and Geometry, Progress in Mathematics, v. 35, Birkhauser, Boston, 1983, 67-107.

[58] S. Ramanujan, Modular equations and approximations to π, Collected Papers, Cambridge, 1927, 23-39.

[59] A. Weil, Elliptic Functions According to Eisenstein and Kronecker, Springer, 1976.

[60] C.L. Siegel, Zum Beneise des Starkschen Satzes, Invent. Math. 5 (1968), 180-191.

[61] G.V. Chudnovsky, Padé approximations to the generalized hypergeometric functions I, J. Math. Pures Appl., Paris, 58 (1979), 445-476.

[62] G. Shimura, Automorphic forms and the periods of Abelian varieties, J. Math Soc. Japan, 31 (1979), 561-579.

[63] P. Deligne, Cycles de Hodge absolus et périodes des intégrales des varietés abéiennes, Bull. Soc. Math. de France, Memoire, No 2, 1980, 23-33.

[64] G. Shimura, Introduction to the Arithmetic Theory of Automorphic Forms, Princeton University Press, 1971.

[65] R. Morris, On the automorphic functions of the group $(0,3;l_1,l_2,l_3)$, Trans. Amer. Math. Soc., 7 (1906), 425-448.

[66] K. Takeuchi, Arithmetic triangle groups J. Math. Soc. Japan, 29 (1977), 91-106.

[67] H.P.F. Swimerton-Dyer, Arithmetic groups, in Discrete Groups and Automorphic Functions, Academic Press, 1977, 377-401.

[68] G.V. Chudnovsky, Algebraic independence of values of exponential and elliptic functions, Proceedings of the International Congress of Mathematicians, Helsinki 1979, Acad. Sci. Fennica, Helsinki, 1980, v.1, 339-350.

[69] G.V. Chudnovsky, Contributions to the Theory of Transcendental Numbers, Mathematical Surveys and Monographs, v. 19, Amer. Math. Soc., Providence, R.I., 1984.

[70] C.H. Clemens, A Scrapbook of Complex Curve Theory, Plenum, 1980.

[71] Y.I. Manin, Algebraic curves over fields with differentiation, Izv. Akd. Nauk. SSSR, Ser. Mat. 22 (1958), 737- 756.

[72] Y.I. Manin, The Hasse-Witt matrix of an algebraic curve, ibid., 25 (1961), 153-172.

[73] B. Gross, N. Koblitz, Gauss sums and the p - adic Γ- function, Ann. Math., 109 (1979), 569-581.

[74] D.V. Chudnovsky, G.V. Chudnovsky, Sequences of numbers generated by addition in formal groups and new primality and factorization tests, Adv. Meth. 7 (1986), 385-434.

[75] P. Henrici, Applied and Computational Complex Analysis, v. 3, John Wiley, 1986.

[76] A. Gerasoulis, M. Grigoriadis, L. Sun, A fast algorithm for Trummer's problem, SIAM J. Ser. Stat. Comput., 8 (1987), s135- s137.