Computer Assisted Number Theory with Applications

D.V. Chudnovsky*), G.V. Chudnovsky*)

Department of Mathematics
Columbia University
New York, NY 10027

Introduction. In this lecture we describe our visions of computer algebra facilities that can be applied in many areas of Number Theory. We describe the design of some of the algorithms that are already used in the development of computer algebra systems. One of the key components of interest to us is the power series facility, particulary for the solution of linear differential equations. Special topics include the determination of monodromy groups and continued fraction expansion. A variety of other applications of computer algebra systems in Number Theory are presented too.

In modern Number Theory, particularly Algebraic Number Theory, the central role, traditionally occupied by arithmetic and analytic computations, has now shifted towards computations of algebraic geometry, especially computations with Abelian varieties. We describe in §1 an ideal facility within a computer algebra system ("Abelian varieties calculator"), that could allow interactive computations and describe the current state of its development. Most of the algorithms and results of this lecture are related to the development of algebraic facilities of computer algebra systems, particularly that of SCRATCHPAD II (IBM). Abelian varieties (elliptic curve computations) appear vividly in modern methods of primality testing and factorization, see §9. One of our main interests is the study of the transcendental part of Abelian varieties computations, particularly, periods of Abelian integrals and algebraic relations between them. These transcendental studies are a part of a more general look at monodromy groups of linear

*) This work was supported in part by NSF DMS-8409626 and the U.S. Air Force AFOSR-81-0190.

differential equations. This point of view allows us to examine simultaneously the uniformization problem for Riemann surfaces (the criterion of Fuchsianity of a monodromy group of a Fuchsian second order linear differential equation). Our main tools for this are power series manipulations with solutions of algebraic and linear differential equations. The problem of the computation of power series expansions of algebraic functions is discussed in §2 and in §3 we consider the Frobenius method of constructing regular expansions of solutions of linear differential equations. Power series methods are used in §4 for the (numerical)analytic continuation of solutions of linear differential equations everywhere on their Riemann surfaces. The crucial problem is the optimal choice, for a given precision of computations, of sides of a polygon, homotopy equivalent to a given path, the analytic continuation along which has the lowest algebraic complexity. Some recipes are very simple (e.g. analytic continuation along the circle around a singularity should proceed along the sides of a regular 17-gon). The continued fraction expansion of algebraic functions are apparently easier to compute than power series expansions. We touch upon this subject and the θ-function representations of elements of the continued fraction expansions in §5. The computation of the N-th element of the continued fraction expansion of a hyperelliptic (or an ultraelliptic $y(x) = \prod_i P_i(x)^{k_i/n_i}$) function $y(x)$ requires at most $O(\log N)$ unit cost operations. This algorithm and the analytic continuation algorithms of §4 are sequential, and often are the best possible. Significant improvement in performance can be achieved only using parallelization. E.g. in order to compute N terms of an algebraic function one needs $O(\log N)$ parallel steps with N processors, cf.§6. Analytic continuation of solutions of linear differential equations leads immediately to an efficient method of computation of elements of monodromy and Galois groups of linear differential equations. We compare different methods of computations of monodromy groups in §7. An immediate arithmetic application of the study of direct and inverse monodromy problems is the arithmetic Galois problem of the construction of a Galois extension of a rational function field $\mathbb{Q}(t)$ with a given Galois group G. The theory here is based on the study of rigid groups following Belyi [40], Matzat [37], Thompson [38]. The monodromy group computations were one of the primary objectives of our work on algorithms of computer algebra. We have developed and implemented a varity of these algorithms, designed for the solution of the direct (computation of the Galois group given a differential equation) and the inverse (determination a differential equation with a given Galois group) monodromy and Galois problems. This package, RIEMANN, is designed for computer algebra interaction and numerical realization in FORTRAN on different mainframes. The monodromy computations for rank one linear differential equations over algebraic curves allow for fast computations of periods of Abelian integrals of all kinds. The description of (linear integral) relations between periods of Abelian integrals is one of the best approaches to the classical problem of the reduction of Abelian integrals to those of lower genra. This problem is studied in §8 from algebraic and transcendental points of view. Algebraic approaches based on the analysis of the torsion of a divisor of a differential (or based on the mod p properties of the power series expansions of algebraic functions via the Grothendieck conjecture [46]) are well suited for comprehensive computer algebra systems, while transcendental methods are easier to realize numerically. The transcendental method of solving the reduction problem (based on the determination of $\mathbb{Z}$-relations between the elements of a Riemann period matrix) is based on multiprecision calculations of periods of Abelian integrals and is a part of our RIEMANN package. In §10 we present some applications of a formal group technique to Tate's problem, following [46], [52] and to primality and factorization testing. Formal groups associated with elliptic curves became recently an important tool in algebraic topology and in §10 we present one explicit formula for important characteristic classes in terms of elliptic modular forms of level 2 which were found using computer algebra power series manipulations. The arithmetic of the monodromy groups of linear differential equations is discussed in §11. The crucial problem here is the transcendence of elements of monodromy matrices of a linear differential equation with coefficients from $\bar{\mathbb{Q}}(x)$ (see Problems 11.1 and 11.2). For first order linear differential equations this problem already includes the transcendence problem for periods of Abelian integrals. For second order linear differential equations practically nothing is known (unless the monodromy group is a commutative one), and we propose to study the monodromy (Fuchsian) groups uniformizing algebraic curves, particularly punctured tori, defined over $\bar{\mathbb{Q}}$. The punctured tori case, the first case in the uniformization theory examined by Poincaré and Klein [30], [66] is already a highly nontrivial one and our numerical efforts have been concentrated on it. Apart from the 4 known cases [67], when the accessory parameter was algebraic for a tori defined over $\bar{\mathbb{Q}}$, we did not find in the course of our search any other ones and it is possible that other values of accessory parameters are transcendental. As for results, rather than experimental observations, we refer to Theorem 11.3 for the transcendence result for the monodromy group elements of the globally nilpotent Fuchsian equation. In §12 monodromy groups of rank 2 linear differential equations are examined from the point of view of their rational approximations and continued fraction expansions. We describe the monodromy group of nonhomogeneous linear differential equations associated with a given homogeneous one, sequences of rational approximations to their elements and the relationship with the Apéry method of approximating $\zeta(2)$ [61], [69]. In §13 we describe different numerical methods of computations of elements of the monodromy group for rank 2 differential equations, especially of second order equations with 4 singularities (Heine or generalized Lamé equations). Particular attention is devoted to the new continued fraction expansions and orthogonal polynomials depending on the accessory parameters that uniformly approximate elements (traces) of the monodromy matrices.

We want to acknowledge the help of the Computer Algebra Group of the T.J. Watson Research Center (IBM), particularly of R. Jenks and B. Trager. Interaction with the SCRATCHPAD II system being developed by this group was and is a tremendous inspiration in our work.

§1. Abelian Varieties Calculator.

One would like (at least we would like) to have a portable, easy-to-use, advanced calculator, which would allow computations with (and on) curves and Abelian varieties with the same ease as, say, pocket HP calculator deals with elementary functions, and the existing computer algebra systems deal with elementary algebra. At the present stage of our interests we would like this calculator to be able to perform the following functions:

1) To find nonsingular models of curves and to determine differentials of the first and the second kind;

2) To determine the Riemann surface of a curve and to compute (with multiple precision) the Riemann matrix corresponding to this curve;

3) To determine the monodromy (Galois) group of a Riemann surface and to be able to construct Riemann surfaces with a given Galois group;

4) To be able to determine rational functions on a Riemann surface having a given divisor (of poles);

5) To have a uniformization of a Riemann surface of genus g by means of rational $(g = 0)$, elliptic $(g = 1)$, and Fuchsian functions $(g > 1)$;

6) To compute Riemann's θ-functions of an algebraic curve and Prym functions; to obtain a uniformization of the Jacobian of an algebraic curve by means of ratios of θ-functions;

7) To have an explicit (numerical and algebraic) solution to Jacobi inverse problem, and to be able to determine the θ-divisor via the theory of surfaces of double translation;

8) To have an implementation of an algorithm for an effectivization of Abel's theorem, and an explicit algebraic expressions for a group law on a Jacobian of a curve, whenever the equation for the curve is given;

9) To be able to compute values of arbitrary g-dimensional θ-functions, particularly multi-precision and fast computation of their values at $(\bar{z},T)$ for an arbitrary point $\bar{z} \in \mathbb{C}^g$ and at a point of a Siegal space $T \in \mathfrak{S}_g$ (i.e. for any Riemann period matrix);

10) To realize the law of addition on an arbitrary Abelian variety

using θ-functions with different sets of characteristics;

11) To be able to compute Schottky conditions on a Riemann period matrix to arise from a Riemann surface (classical conditions for small g and conditions arising from the higher Kadomtzev-Petviashvily equations);

12) To be able to determine the factors of the Jacobians, and reducibility of various Abelian integrals to lower genra;

13) To find minimal arithmetic models for elliptic curves and Abelian varieties; to determine the structure of bad reductions;

14) To be able to compute heights on Abelian varieties and to have the realization (conditional on the Birch-Swinnerton-Dyer conjecture) of algorithms determining the basis of a Mordell-Weil group of an Abelian variety;

15) To perform diophantine analysis on Abelian varieties, particularly to find all integral points on elliptic curves and on curves of genus $g > 1$ (conditionally on the Birch-Swinnerton-Dyer conjecture);

16) To do archimedian and p-adic analysis of L-functions associated with elliptic curves and Abelian varieties and to give (numerically close) expressions for special values of L-functions.

Such a sophisticated calculator exists so far only on paper, and is not likely to appear on the market in the next few years. Nevertheless it is being built up piece by piece. The backbone of this calculator is the power series manipulation facility,that we are developing, and computer algebra systems (in LISP and SCRATCHPAD II of IBM).

Among features described above, 1), 3), 4) are being realized in SCRATCHPAD II; 2) is realized for hyperelliptic curves and arbitrary curves of low genus; 6) and 8) are realized for hyperelliptic curves; for 5) we have various programs that do not yet form an automatic package; 7) is only partially realized; 9) is realized numerically for low genra; 10) is realized only for dimensions 1 and 2; 12) is realized in various situations for curves over constant and function fields; 13) and 14) exist only for elliptic curves; 11), 15)-16) are not yet developed.

Among the related facilities that we are working on and are reporting below is a facility to compute in various ways (transcendentally and algebraically) the monodromy group of differential and algebraic equations and the solution of the inverse monodromy problem. Some of these programs (particularly aimed at the inverse monodromy problem) are written in FORTRAN for faster execution in a single-or double-precision modes. Other programs require the interface with a computer algebra system.

§2. Power Series Expansions of Algebraic Functions in Computer Algebra.

An important part in any computer algebra system is occupied by a power series package. Typically this package allows one to perform algebraic operations with power series and expands elementary functions around nonsingular points into power series. More sophisticated systems (say, MACSYMA) have Puiseux expansions facility, can compose power series and analyze the character of singularities. The power series facility is important in applications because it is the only way to solve various differential equations that do not have closed form solutions. We found that power series manipulations are important in various mathematical problems. To name but a few: 1) Power series serve as a basis for the construction of various rational (Padé) approximations to solutions of algebraic or differential equations. This way one can construct explicit rational approximations to functions and their values-an important task in transcendental number theory.

2) Power series over $\bar{\mathbb{Q}}$ or $\mathbb{Q}_p$ play an important role in the efficient computation of algebraic numbers and functions (including, e.g. construction of modular equations).

3) Power series expansions and analytic continuation based on them, provide a unified way to study the Galois groups of linear differential equations in algebraic function fields, support an algorithm to determine the reducibility of Abelian integrals, and allow one to study the definite integrals of special functions.

4) Power series manipulations are indispensable in the study of formal groups. In connection with this one can mention the modular function algebra, where power series manipulations are crucial (e.g. in proving of new identities of Rogers-Ramanujan type, see Andrews [22]).

One of our interests in the development of the power series facility for SCRATCHPAD II lay in the opportunity to perform very large scale jobs involving power series with dozens of thousands of terms.

Because of this, the focus of our study was the prepration of the least complex algorithms for power series expansions and power series manipulations. A crucial test for a power series package is the ability to manipulate fast with functions that arise by iterations of the following operations: a) solutions of algebraic equations; and b) solutions of (linear) differential equations.

To perform this task fast one needs fast algorithms that computes N first (or the N-th) coefficients in the Puiseux or power series expansion of an algebraic function. We refer to Kung-Traub [4] and Knuth [6] for the description of existing algorithms based on the Newton method that require at least $O(N \log N)$ operations, even if the fast multiplication methods are used.

We had implemented an algorithm that requires only $O(N)$ operations and $O(1)$ storage to compute the N-th coefficient in the power series expansion of an algebraic function.

Remark: The constant in $O(\cdot)$ depends on the total degree of an algebraic equation. However, when one deals with arbitrary precision rational arithmetic the constant in $O(\cdot)$ will start to depend on the size of the coefficient too (as the memory requirements to store one large number depends on its size). In one important case, when one is interested only in mod p values of the coefficients, the constant $O(\cdot)$ will be $O(\log p)$ since all numbers can be assumed to be at most $p-1$.

The algebraic function power (and Puiseux) series expansion algorithm, described in detail in our paper [8], is based on the reduction of an algebraic equation satisfied by an algebraic function, to a (Fuchsian) linear differential equation satisfied by all branches of a given algebraic function. As it turned out, the problem of power series expansion for (Fuchsian) linear differential equation is an easy one, solvable via the Frobenius method, see the next section for details.

Several important theoretical questions on the complexity of power series computations are left open. Among them are the following:

1) Is the complexity of the computation of N-th coefficient of an algebraic function always "exponential," i.e. it takes $O(N)$ operations? (It seems to be so, even for the simplest functions like $\sqrt{1-4x}$ at $x = 0$, even if computations are conducted mod n for a

composite n--because otherwise the factorization problem would be simple).

2) What is the minimal complexity of the computation of N-th coefficient of a power series expansion of an algebraic function mod p for a fixed (large) prime p?

This problem is connected with the congruences satisfied by the expansions of differentials on algebraic curves (known as Atkin-Swinnerton-Dyer congruences for elliptic curves, see [27]). The most interesting class of algebraic functions is, of course, the class of radicals, particularly the square roots of polynomials: $\sqrt{P(x)}$. Cubic polynomials (the elliptic function case) represent an extremely interesting sub-class, for which we don't know the answer to 2). Classican congruences of Schur type (for the Legendre polynomials) allow us to compute fast the N-th coefficient mod p, when p is fixed (and small). It is reasonable to conjecture that in the situation of Problem 2) one needs at most $O(L(p)\log N)$ operations, where $L(p) = \exp(\sqrt{\log p \log \log p})$ at least for hyperelliptic algebraic functions. This conjecture is partially verifiable for primes p of special form (with $p \pm 1$ being a power of 2). The Problem 2) is not unrelated to the discrete logarithm problem and to the factorization problems discussed below.

The complexities discussed in this section are the complexities of sequential algorithms; the corresponding parallel algorithms are discussed in §6.

§3. Solution of (Linear) Differential Equations in Power Series.

Linear differential equations with analytic function coefficients are solvable in terms of analytic functions regular in the neighborhood of any point in the extended complex plane, which is not a singularity of one of its coefficients. This result and its generalizations to solutions of linear differential equations that have at most algebraic or logarithmic singularities is usually attributed to Fuchs [1]. The analyticity of solutions at regular (regular singular) points allows one to expand these solutions in power series convergent in the neighborhood of these points. The first explicit algorithm of construction of a basis of regular solutions of linear differential equations in the neighborhood of a regular or regular singular point was described by Frobenius [3] and his algorithm is known as the method of Frobenius. This method is used in computer algebra systems, see [7]. The implementation of the Frobenius method aimed for the SCRATCHPAD II is presented in our report [8]. It follows from [8] that to compute N coefficients of a regular expansion of a solution of a linear differential equation at a regular (regular singular) point one needs at most $O(N)$ operations and $O(N)$ storage space, whenever the expansions up to the order $N + O(1)$ of the coefficients of this linear differential equation are known. These computations are "on-line" in the Kunth terminology, i.e. to compute N-th coefficients c_N of the expansion $y(x) = (x - x_0)^{\alpha}\cdot\Sigma_{N=0}^{\infty} c_N(x-x_0)^N$ of a solution $y(x)$ one uses a recurrence formula

$$(3.1) \qquad c_N = \sum_{i=0}^{N-1} c_i A_{N,i},$$

where $A_{N,i}$ are explicitly expressed in terms of coefficients of the power series expansions of coefficients of a linear differential equations and rational functions of i and N.

For applications the most important class of linear differential equations is that of equations with rational function coefficients. For this class of equations the complexity results above can be considerably improved. Namely, the number of operations needed to compute the N-th coefficient in the regular expansion of a solution of a linear differential equation, is $O(N)$ with <u>only</u> $O(1)$ storage.*) The constant in $O(\cdot)$ depends on the order of a linear differential equation and degrees of its polynomial coefficients. The key to this computational method lies in the recurrence (3.1) for the coefficients c_N, that becomes the recurrence of the finite order. We present this recurrence explicitly since it is referred to in the text. Let us consider a scalar linear differential equation of n-th order

$$(3.2) \qquad \sum_{i=0}^{n} a_i(x)y^{(i)}(x) = 0,$$

with rational function coefficients. We look at the expansion of a fundamental system of solutions of (3.2) in the neighborhood of a point $x = x_0$, which is either regular or regular singular for (3.2).

*)One algorithm needs $O(N)$ additions and $O(\sqrt{N}\log N)$ multiplications.

According to the Fuchs criterion [1], [2] this means that (3.2) can be represented in the form

$$\sum_{i=0}^{n} b_i(x)(x-x_0)^i y^{(i)}(x) = 0, \tag{3.3}$$

for polynomials $b_i(x)$: $i = 0,\ldots,n$ and $b_n(x_0) \neq 0$. The solutions $y = y(x)$ of (3.3) have, in general, the form

$$y(x,\alpha) = (x-x_0)^{\alpha} \cdot \sum_{N=0}^{\infty} c_N(\alpha)(x-x_0)^N, \tag{3.4}$$

where the coefficients $c_N = c_N(\alpha)$ satisfy the recurrence of the form

$$\sum_{j=0}^{\max(N,d)} c_{N-j} \cdot f_j(\alpha+N-j) = 0 \tag{3.5}$$

where $d = \max\{\deg(b_i(x)): i = 0,\ldots,n\}$ and the coefficients $f_j(\alpha)$ are defined as:

$$\alpha(\alpha-1)\ldots(\alpha-n+1)b_n(x) +\ldots+ \alpha b_1(x) + b_0(x) \stackrel{\text{def}}{=}$$

$$f_0(\alpha) + (x-x_0)f_1(\alpha) +\ldots+ (x-x_0)^d f_d(\alpha).$$

The exponents α in (3.4) are determined as roots of the indicial equation $f_0(\alpha) = 0$. [There are n such roots whenever $x = x_0$ is a regular point of (3.2); otherwise there might be fewer than n linearly independent solutions of (3.2) of the form (3.4)]. If $x = x_0$ is a regular singularity and there are roots of the indicial equation differeing by integers, then there might occur additional logarithmic terms $\log^i(x-x_0) \cdot \Sigma_{N=0}^{\infty} c_{N;i}(x-x_0)^N$ in the expansions (3.4). The coefficients $c_{N,i}$ are determined by the recurrences of the form (3.5), but in the inhomogeneous form; for details see [8]. For a regular $x = x_0$, the solution of recurrence (3.5) is uniquely determined by the initial conditions of $y(x)$. We can represent the recurrence (3.5) as

$$c_N = \sum_{i=1}^{n} A_{N,i} c_{N-i}, \tag{3.5'}$$

where $A_{N,i} = P(N;i)/Q(N)$ are rational functions of N and i. The degrees of polynomials $P(N;i)$ and $Q(N)$ depend <u>only</u> on the order of a linear differential equation. A more important parameter is the length r of the recurrence (3.5') known as <u>a rank</u> of the linear differential equation at a given point. A rank never exceeds the sum of the order of the differential equation and the maximal degree of its polynomial coefficients. However, often the rank is much smaller. For example, all generalized hypergeometric equations of arbitrary orders have rank one at their regular singularities. Similarly, for the Fuchsian second order linear differential equations of the second order the rank at an arbitrary regular singularity never exceeds the number of singularities minus 2.

Expansion of algebraic functions described in [8] is based on power series algorithms for Fuchsian equations that are derived from the algebraic equations [2], [8].

Regular expansions of solutions of linear differential equations have to be substituted by asymptotic series expansions if the point of expansion is an irregular singularity (i.e. does not satisfy the Fuchs conditions and equation (3.2) cannot be represented in the form (3.3)). Solutions in the neighborhood of an irregular singularities are usually expressed in terms of normal and subnormal series studied by Poincaré. Normal and subnormal solutions in the neighborhood of, say, $x = \infty$ have the form $e^{Q(x^{\alpha})} \cdot f(x^{-\alpha})$, where $Q(\cdot)$ is a polynomial, and $f(.)$ is an asymptotic power series. These expansions converge in sectors at $x = \infty$ with the connection formulas known as Stokes formulas. When normal and subnormal expansions exist, and this can be determined effectively, the algorithm for the computation of coefficients in the asymptotic series is very similar to the Frobenius method, and satisfies the same requirements for the complexity and storage as in the computations of regular expansions. For a general irregular singularity, instead of recurrences, one can use Poincaré-Koch method based on infinite Hill determinants that determine the Laurent expansion of a solution convergent in the disk with the puncture at irregular singularity, see below in connection with discussion of the Hill method. This method [24] [26] allows us to compute Stokes' multipliers numerically. Stokes' multipliers do not belong to a monodromy group of a differential equation, but to its Galois group. Similar to monodromy matrices, the explicit expressions for Stokes multipliers are known in a few cases--these are the confluent hypergeometric equations, see [25].

For nonlinear differential equations methods of power series expansions of their solutions were sketched in [9], based on FFT and the Newton method. We use the linearization technique that allows us to reduce the power series computation of solutions of nonlinear (algebraic) differential equations to: a) solution of linear differential equations, b) elementary operation with power series and c) the Newton method. Algorithms of [9] assure that this can be done in at most O(N log N) operations.

§4. Optimal Analytic Continuation of Solutions of Linear Differential Equations.

The fast multiple precision computation of power series expansions of solutions of linear differential equations allow one to analytically continue the solution of a linear differential equation with given initial conditions to an arbitrary point of the Riemann surface of this solution. This procedure is not unlike numerical integration (but in the complex plane); the difference is the multiple precision that we require in this process at every step. As we show, the sizes of steps in this analytic continuation process are relatively large in sharp contrast with the standard numerical integration procedure.

To describe the analytic continuation for solutions of linear differential equations precisely, it is easier to deal with linear differential equations in the matrix first order form:

$$\frac{d}{dx} Y = A(x)Y. \tag{4.1}$$

Let $Y(x;x_0)$ be a $n \times n$ matrix solution of (4.1) normalized at $x = x_0$:

$$Y(x;x_0)\big|_{x=x_0} = I_n,$$

for a unit matrix $I_n = (\delta_{ij})_{i,j=1}^{n}$. The basic rule of analytic continuation is the superposition formula, see, say [10], according to which

$$Y(x;x_1)\cdot Y(x_1;x_0) = Y(x;x_0) \tag{4.2}$$

for any three points x_0, x_1, x in $\mathbb{CP}^1$. The superposition formula gives the following simple chain rule of analytic continuation of an arbitrary solution of (4.1) along any path γ in $\mathbb{CP}^1$. Let us assume that γ is not passing through any of the singularities of (4.1). Let x_0 be the initial point of γ and x_{fin} be its end-point (they can coincide). Then, by choosing m + 2 vertices $x_0, x_1, \ldots, x_m, x_{m+1} = x_{fin}$ on γ, we can replace the process of analytical continuation of a normalized solution $Y(x;x_0)$ along γ from x_0 to x_{fin} by the process of successive solution of (4.1) with new initial conditions:

$$Y(x_{fin};x_0) \text{ (the analytic continuation of } Y(x;x_0) \text{ from } x_0 \text{ to } x_{fin} \text{ along } \gamma) \underset{\gamma}{\mapsto} Y(x_{fin};x_m)\cdots Y(x_2;x_1)Y(x_1;x_0). \tag{4.3}$$

In order to apply this chain rule, one has to be sure that each of the factors, $Y(x_{i+1};x_i)$ is defined nonambigously. For this it is sufficient to assume that x_{i+1} lies in the disk with the center x_i and the radius of this disk is smaller than the radius of convergence of $Y(x;x_i)$. The radius of convergence of $Y(x;x_i)$ is always bounded by a distance from x_i to the nearest singularity of a linear differential equation. Since the singularity set is discrete, there is always a finite set of m + 2 points on γ, so that the analytic continuation along γ is equivalent to the analytic continuation along the polygon formed with these m + 2 points as vertices. To continue analytically the solution along the edge $\overrightarrow{x_i x_{i+1}}$ of this polygon, one has to construct only the power series expansion of $Y(x;x_i)$ with sufficiently many terms so that the evaluation of $Y(x;x_i)$ at $x = x_{i+1}$ be close to the actual one within a given precision. From the point of view of minimal complexity the main problem is to determine the minimal number of m + 2 points x_i and their positions, for which the number of operations necessary to complete the analytic continuation within a given precision is minimal. This leads to an interesting extremal problem which we solve explicitly below in a few most important cases, e.g. when γ is a line or a circle (the only two basic elements needed). As it turned out, even in general, the minimal number of m + 2 points <u>does not depend on the chosen precision</u> but depends only on the positions of singularities of a linear differential equation and on the path γ. Moreover, this number is always bounded (for a given set of singularities) by the function of logarithm of the total length of γ. Consequently:

<u>Corollary</u>: One can compute the value of a solution of arbitrary linear differential equations with precision M (i.e. with M significant

digits) at an arbitrary point x on the Riemann surface of this function in at most $O(M\cdot\log(\|x\|+1))$ operations, where $\|x\|$ is a distance from x to the base points x_0 of the initial integration.

Remark 4.1: Modifications of our method allow an improvement in the speed of computations from $O(M\log(\|x\|+1))$ to $O(\log(M+1)\cdot\log(\|x\|+1))$ for a large class of equations. This class includes all algebraic functions, where the constant in $O(\cdot)$ depends on the differential equation satisfied by these functions. This number of operations is the best possible.

Remark 4.2: The superposition formula can be considered as an analytic expression of the law of addition in the formal Lie group generated by the natural action of a differential equation. This law of addition often takes a familiar form; e.g. for the equation $y' = 1/x$, the superposition law is simply the addition formula for the logarithmic function. Similarly, one finds immediate relationship with the Abel theorem for elliptic integrals of various kinds. Continuing this similarity, one realizes that our method of computations of solutions of linear differential equations at points outside their natural domain of convergence generalizes classical (going back to Gauss) methods of computations of logarithms, inverse trigonometric functions and elliptic integrals known under the name of Borchardt's algorithms. These methods should not be confused however with the much faster (quadratically) convergent Gauss arithmetic-geometric mean algorithm, that computes only complete elliptic integrals, i.e. periods of elliptic integrals of the first kind. The discussion of a variety of Borchardt-Gauss algorithms for computations of elliptic integrals of all kind see Carlson [11]. For applications of Gauss' algorithms to fast multiple-precision evaluations of elementary functions see Brent [12].

Now we formulate the problem of the optimal choice of the inscribed polygon in the analytic continuation with a given precision as a variational problem, and give simple answers for a few critical geometries of a path.

We assume that the linear differential equation has rational function coefficients and either has matrix form (4.1) with $A(x) \in M_n(\mathbb{C}(x))$, or else is a scalar n-th order linear differential equation with polynomial coefficients:

$$\sum_{i=0}^{n} a_i(x)y^{(i)}(x) = 0, \tag{4.4}$$

$a_i(x) \in \mathbb{C}[x]$: $i = 0,\ldots,n$; $a_n(x) \not\equiv 0$. Let us denote by $S = \{a_1,\ldots,a_{k+1}\} \subset \mathbb{CP}^1$ the set of all singularities of a linear differential equation: in the case (4.1) these are the poles of all rational function entries of $A(x)$; in the case (4.4) these are the zeroes of $a_n(x)$ and, possibly, ∞, if it is a singularity of (4.4). Let us fix a path γ in $\mathbb{CP}^1\backslash S$. There are two natural formulations of optimal analytic continuation along γ described above.

I) One fixes γ having initial point x_{in} and its end point x_{fin}. We want to find a number m and points $x_0 = x_{in}, x_1, \ldots, x_m, x_{m+1} = x_{fin}$ lying on γ such that the computation of power series expansions of a given solution at x_i and their evaluations at $x = x_{i+1}$ consecutively for $i = 0,\ldots,m$ requires the minimal number of operations for a given precision of calculations.

II) Since analytic continuation along γ depends only on the homotopy class of γ in $\pi^1(\mathbb{CP}^1\backslash S)$, one can ask in I) to find a polygon $\Delta = \overrightarrow{x_0x_1}\ \overrightarrow{x_1x_2} \ldots \overrightarrow{x_mx_{m+1}}$ with vertices $x_0,\ldots,x_{m+1}$ equivalent to the path γ in $\pi^1(\mathbb{CP}^1\backslash S)$, and for which the process of consecutive computation of power series expansions of a given solution at x_i and their evaluations at x_{i+1} for $i = 0,\ldots,m$ requires the minimal number of operations for a given precision of calculations.

Our main interest lies with Problem I. We do not know yet a complete answer to Problem II, when the number $k + 1$ of singularities exceeds 3. Problem II seems to be related to a variety of problems of sets of minimal capacity on Riemann surfaces.

To solve these problems one has to determine the number of operations needed to compute a power series expansion at, say, $x = x_0$, in order to obtain a value of the solution (and its derivatives up to the order $n - 1$ for the equation (4.4)) at, say, $x = x_1$, within a given precision of computations. We fix the precision as a sufficiently large integer M, so that the computations have to be carried out up to the order $\varepsilon \overset{\text{def}}{=} O(10^{-M})$. Power series (Taylor) expansions of solutions of (4.1) or (4.4) are computed via the finite-term recurrences satisfied by coefficients of these expansions. We concentrate on the case (4.4), where the expansions at $x = x_0$ are given in (3.4) with explicit recurrences in (3.5).

Remark: In our implementations of (3.4)-(3.5) we prefer to compute $c_N(\alpha)\cdot(x-x_0)^N$ recursively, instead of computing $c_N(\alpha)$ and $(x-x_0)^N$ separately. Differentiating (3.4), one determines the derivatives of $y(x)$. In fact, all the coefficients $c_N^{(i)}$ of $y^{(i)}(x) = \Sigma_{N=0}^{\infty} c_N^{(i)}(x-x_0)^i$ for $i = 1,\dots,n-1$ are computed as a part of the recurrent scheme (3.5).

The problem of opitmal analytic continuation of $y(x)$ from x_0 to x_1 with a given precision is equivalent to the problem of bounding the number, D, of terms $c_N\cdot(x-x_0)^N$ in the expansion (3.4) that one has to compute to bound the error in the evaluation of new initial conditions of $y^{(i)}(x)$ at $x = x_1$ $(i = 0,\dots,n-1)$ by $\varepsilon(= O(10^{-M}))$:

(4.5) $$\max_{i=0,\dots,n-1} \left|\sum_{N=0}^{D} c_N^{(i)}(x_1-x_0)^i - y^{(i)}(x_1)\right| \ll \varepsilon.$$

The radius of convergence of series (3.4) is equal to the distance from x_0 to the nearest singularity from S. Namely, let $\mathrm{dist}(x_0,S) \stackrel{\text{def}}{=} \min_{a_i \in S}|x_0-a_i|$. Then we have

(4.6) $$\frac{1}{N}\log|c_N| \le -\log \mathrm{dist}(x_0,S).$$

Moreover, in general (e.g. when all the numbers $|x_0-a_i|$ are distinct for $i = 1,\dots,k+1$) and for a generic solution $y(x)$ one has the (asymptotics) expansion

(4.7) $$|c_N| = N^{\nu}.\mathrm{dist}(x_0,S)^{-N}.(\alpha_0 + \frac{\alpha_1}{N} + \dots)$$

as $N \to \infty$. Here ν is an explicitly computable (rational) number. Consequently, to achieve the error bound (4.5) for a given precision M one has to compute D terms in power series (3.4) for D bounded by (ε is sufficiently small):

(4.8) $$D \ge \frac{1}{\log_{10}\left(\frac{\mathrm{dist}(x_0,S)}{|x_1-x_0|}\right)}\cdot M\cdot(1+O(1)).$$

For a given D, the number of operations necessary to evaluate D terms in the power series expansion (3.4) can be estimated from the recurrence (3.5). Denoting this number by #D, we get the following (crude) bound:

(4.9) $$\#D = O_{n,d}(D) \leq O(n^2 dD).$$

As a consequence of (4.8), (4.9) one needs at most

$$O(M/\log(\frac{\mathrm{dist}(x_0,S)}{|x_1-x_0|}))$$

operations to evaluate initial conditions of a given integral $y(x)$ at $x = x_1$ with a given precision M. At the next step of analytic continuation from x_1 to x_2 one takes the approximate initial conditions computed in (3.5) with an error ϵ and evaluates a new power series expansion at $x = x_1$ at the next point $x = x_2$ with the same error ϵ. In this process the error can increase only linearly with the number of steps in the analytic continuation process, whenever the values of functions stay bounded. For this it is sufficient to assume that $\mathrm{dist}(x_i,S)$ is bounded from below and we have $\frac{|x_{i+1}-x_i|}{\mathrm{dist}(x_i,S)} < 1 - \delta$ for a fixed $\delta > 0$.

Consequently, for the fixed precision M the Problem I is reduced to the following extremal problem:

<u>Problem I'</u>: For a given path γ, find the minimum:

$$\min_m \cdot \min\{I(x_0,\ldots,x_{m+1}) : x_0 = x_{in}, x_{m+1} = x_{fin}, x_i \in \gamma,$$

$$|x_{i+1}-x_i| < \mathrm{dist}(x_i,S)\}, \text{ with } I(x_0,\ldots,x_{m+1})$$

$$= \sum_{i=0}^{m} 1/\log(\frac{|x_{i+1}-x_i|}{\mathrm{dist}(x_i,S)}).$$

A source of complications is a non-analytic function $\mathrm{dist}(x_0,S)$. Problem I' can be easily solved for paths γ that lie in the domains, where $\mathrm{dist}(x,S) = |x-a_i|$ for a fixed a_i. Two crucial examples are the circle around the singularity and a straight line moving away from a given singularity. In both cases we found m, x_i and the value of the minimum.

<u>Proposition 4.1</u>: Let γ be a straight path from x_{in} to x_{fin}, where x_{in} is not a singularity and for all points on γ, there is a single $a_i \in S$, which is the closest element of S. Without loss of generality we can assume $x_{in} = 1$, $a_i = 0$ and x_{fin} is real > 0. Then the solution to Problem I' has the following forms:

$$x_i = x_{fin}^{i/(m+1)} : i = 0,\ldots,m+1$$

(so that $x_0 = x_{in}$, $x_{m+1} = x_{fin}$). The number m is defined so that $m + 1$ is (non-negative) integer closest to $\ln x_{fin}/\ln \beta$. Here $\beta = 1.318\ldots$ is the solution of a transcendental equation

$$\frac{\ln(\beta-1)}{\ln \beta} + \frac{\beta}{\beta-1} = 0.$$

Proof: First of all for a fixed m we try to minimize the functional $I(x_0,\ldots,x_{m+1}) = \Sigma_{i=0}^{m} \dfrac{1}{\log(\frac{x_{i+1}-x_i}{x_i - 0})}$ with $x_0 = 1$. Differentiating this functional with respect to x_i, one finds consecutively that the solution satisfies $x_{i+1}/x_i = x_i/x_{i-1}$: $i = 1,\ldots,m$. This shows that $x_i = x_{fin}^{i/(m+1)}$: $i = 0,\ldots,m+1$. Thus we have

$$\min_{x_{i-1}<x_i<x_{i+1}} I(x_0,\ldots,x_{m+1}) = \frac{m+1}{\log(x_{fin}^{1/(m+1)}-1)} \overset{\text{def}}{=} J(m).$$

In the last expression one considers m as a variable and minimizes with respect to m. We are left with the transcendental equation: $\ln(\beta-1)/\ln \beta + \beta/\beta-1 = 0$ for $\beta \overset{\text{def}}{=} x_{fin}^{1/(m+1)}$. Its only solution in a given range is $\beta = 1.318\ldots$. This proves Proposition 4.1.

Proposition 4.2: Let γ be a closed circular path encompassing a single singularity as a center. Let us assume that the radius of γ be smaller than a half of a distance from a given singularity to any other one. Then in Problem I' the minimal number $m + 1$ of distinct points of γ (we assume that $x_{in} = x_{fin}$) is 17, and these points form a regular 17-gon inscribed into γ.

Proof: Similar to the proof of Proposition 4.1.

In a sense, Proposition 4.1 and 4.2 give a recipe for an arbitrary analytic continuation, because up to homotopy all paths can be represented as the two kinds covered by Proposition 4.1 and 4.2. This recipe can be often very simple. Consider a case when we continue analytically a solution from a point x_0 near a singularity a_i along a straight path connecting a_i and x_0. The rule of analytic continuation is the following: once x_i is determined, choose x_{i+1} as a further point on this path, the distance from which to a_i is β times the distance of x_i to a_i; with $\beta = 1.318\ldots$. If x_{fin} preceeds x_{i+1}, put $x_{i+1} = x_{fin}$.

§5. Continued Fraction Expansions of Algebraic Functions

Computations of continued fraction expansions, or equivalently, of Padé approximations to functions require, by definition, the computation of power series expansions of these functions. Let us remind the definition of a continued fraction expansion at $x = x_0$ of a function $f(x)$ analytic (or given by a formal power series) at $x = x_0$. Usually, one takes $x_0 = \infty$. If we denote by $[h(x)]_\infty$ a singular part of a function $h(x)$ at $x = \infty$:

$$h(x) = [h(x)]_\infty + h_{-1}/x + h_{-2}/x^2 + \ldots,$$

then the algorithm of the continued fraction expansion of $f(x)$ is the following: $f_0(x) = f(x)$, $a_i(x) = [f_i(x)]_\infty$, $f_{i+1}(x) = (f_i(x)-a_i(x))^{-1}$: $i \geq 0$. This expansion is represented symbolically as

$$f(x) = a_0(x) + \cfrac{1}{a_1(x) + \cfrac{1}{a_2(x) + \ldots}}.$$

It follows from the results of §§2-3 that the computation of N-th element $a_N(x)$ in the continued fraction expansion of an arbitrary algebraic function requires at most $O(N \log^2 N)$ operations and $O(N)$ storage. It might seem unlikely (up to a factor of $\log^2 N$) that these computations can be speeded up since it is well known how difficult it is to compute a continued fraction expansion of a number or a function. Nevertheless, as it turned out, the continued fraction expansions of large classes of algebraic functions are easier to compute than the corresponding power series expansions. For example, we have the following results:

Proposition 5.1: Let $y(x)$ be an algebraic function satisfying quadratic or cubic equations over a rational function field. Then in order to compute N-th elements $a_N(x)$ in the continued fraction expansion of $y(x)$ one needs at most $O(\log N)$ operations. The constant in $O(.)$ depends only on the genus of a function field to which $y(x)$

belongs and on the representation of $y(x)$ in terms of the basis of this field.

The key to the proof of this proposition lies in the representation of partial fractions of the continued fraction expansion of $y(x)$ in terms of θ-functions on a Riemann surface of $y(x)$. Such a representation in the elliptic case belongs to Abel [15] and Frobenius-Stickelberger [16]. In general hyperelliptic case (see particularly [20]) these expressions were derived by H.F. Baker [17], and are now familiar to many as θ-function expressions for "Baker-Akhiezer" eigenfunctions from the theory of the finite band Korteweg-de Vries equations (KdV) or periodic Toda lattices [19]. From the θ-functions representation one derives the expression of $a_N(x)$ in terms of the multiplication formula for θ-functions. This allows for polynomial time (in $O(\log N)$) of computation of $a_N(x)$. We note that the degrees of $a_N(x)$ are always bounded for arbitrary algebraic functions according to our results on the <u>exponent 2</u> in the rational approximation problem for algebraic functions [14]. Explicit representation of elements and partial fractions of continued fraction expansions in elliptic case can be found in [14,§2]. To evaluate these expressions one needs fast evaluation methods for $\psi_n = \sigma(nu)/\sigma(u)^{n^2}$ that follow from various multiplication formulas for θ-functions described in [21]. Cf. below for the discussion of the elliptic divisibility sequence ψ_n.

Polynomial time computations of continued fraction expansions was implemented by us for elliptic and hyperelliptic genus two functions.

Similarly, in the Hermite-Padé approximation problem [13-14] for several algebraic functions, the coefficients of the recurrences satisfied by Padé approximants can be determined in the polynomial time in the following cases: when we Padé approximate simultaneously k functions $f_1(x),\dots,f_k(x)$ that belong to an algebraic function field of degree d with $k = d - 1$, or $k = d - 2$ (cf. [14,§4]).

In any of these cases, we can also determine in a polynomial time (i.e. in $O(\log N)$ operations) the value $R_N(x_0)$ of N-th remainder function for a fixed value $x_0 \neq \infty$, and also the values of N-th Padé approximants at $x = x_0$.

We conjecture that the polynomiality of computations of elements of the continued fraction expansions still holds for arbitrary algebraic functions without restrictions on their degrees. This conjecture holds for all radical functions $y(x) = \prod_{i=1}^{n} P_i(x)^{m_i/k_i}$ and, in general, for all $y(x)$ satisfying Ricatti equations (cf. [14]).

§6. On Parallel Algorithms.

Discussing the complexity problems in computation of power series expansions and continued fraction expansions one should touch upon the construction of parallel algorithms for these computation, and their complexity. In the computation of power series solutions of linear differential equations with rational function coefficients, there are two possibilities for the parallelization. The first approach, an extension of our work in [8], requires the parallel computations with the recurrences determing the coefficients of the power series expansions of solutions. In this approach, in order to compute N terms of power series expansion, one needs a parallel time of $O(\log N)$ with N processors. The precise computation of constants is an interesting problem; these constants depend on the rank and degrees of coefficients of the equation. In the second approach one can use the Newton method for computation of solutions of linear differential equations, following Brent-Kung [9], but in parallel. The parallel running time is again $O(\log N)$.

The first approach using recurrences is particularly easy to parallelize or even vectorize for low ranks. E.g. the rank 2 case is reducible to the famous problems of parallel computations with three-diagonal (Jacobi) matrices, which attracted significant attention in the literature [23].

Fast parallel computations allow also to replace $O(N)$ by $O(\log N)$ parallel steps in Corollary of §4.

Parallel computations of continued fraction expansion is particularly attractive, when elements of the continued fraction expansion are known in advance, or are easy to compute. Clearly, continued fraction expansion of quadratic (radical) algebraic functions falls into the latter category, because of the low complexity of (independent) computation of their elements. One can estimate the total parallel time of the computations of N-th partial fraction of an algebraic function considered in Proposition 5.1 as $O(\log N)$ with the constant in $O(\cdot)$ depending on the genus of a function field for a large N. At this moment we have not implemented this parallel continued fraction algorithm for algebraic functions. However, we took full advantage of vectorization in power series algorithms in FORTRAN programs on supercomputers.

§7. Monodromy and Galois Groups of Linear Differential Equations.

A traditionally transcendental problem in the theory of linear differential equations is a problem of determination of the monodromy group of a differential equation from its coefficients [18], [19]. A closely related problem is that of differential algebra [28], where one wants to determine a Galois group of a (Picard-Vessiot extension corresponding to a) linear differential equation from its coefficients (lying in a differential field). We call these problems direct monodromy and Galois problems for linear differential equations, and we start with precise definitions. In this discussion the coefficients of linear differential equations are always from a subfield of $\mathbb{C}(x)$ (the most interesting case being $\mathbb{Q}(x)$).

The concept of a monodromy group was developed by Riemann [29] to describe the invariants associated with analytic continuation.

Let us start with a linear differential equation

$$(7.1) \qquad a_n(x)y^{(n)} + \ldots + a_1(x)y' + a_0(x)y = 0$$

with rational functions coefficients $a_i(x)$. Let us denote by S the set of all singularities of equation (7.1); these are the singularities (poles) of $a_i(x)$ or zeroes of $a_N(x)$ in the extended complex plane $\mathbb{CP}^1$. Then the analytic continuation of a particular fundamental system of solutions of (7.1) induces a representation of a fundamental group of $\mathbb{CP}^1\backslash S$ in $GL_n(\mathbb{C})$. This representation ("a" monodromy group) is defined as follows. Let $y_1(x),\ldots,y_n(x)$ be a fundamental system of solutions of (7.1). Then the analytic continuation along the closed path γ in $\mathbb{CP}^1\backslash S$ of $\{y_1(x),\ldots,y_n(x)\}$ yields the linear transformation of these solutions:

$$(7.2) \qquad (y_1(x),\ldots,y_n(x)) \underset{\gamma}{\mapsto} (y_1(x),\ldots,y_n(x))M(\gamma)$$

when prolonged along γ.

The matrix $M(\gamma) \in GL_n(\mathbb{C})$ depends only on the homotopy class of γ in $\pi_1(\mathbb{CP}^1\setminus S)$. Also

$$M(\gamma_1\gamma_2) \equiv M(\gamma_1)M(\gamma_2),$$

and the set $\mathfrak{M} = \{M(\gamma)\}$ is a group (a representation of $\pi_1(\mathbb{CP}^1\setminus S)$). A monodromy group $\mathfrak{M}$ of (7.1) depends on the choice of a basis $\{y_1(x),\ldots,y_n(x)\}$. Hence by "the" monodromy group of (7.1) one usually understands a conjugacy class of $\mathfrak{M}$ in $GL_n(\mathbb{C})$.

Let $S = \{a_1,\ldots,a_m\}$. Then a monodromy group $\mathfrak{M}$ is generated by m matrices $M_i = M(\gamma_i)$: $i = 1,\ldots,m$, where γ_i is a clockwise circuit around a_i which does not contain other singular points inside, and with the proper enumeration we have

$$M_1 \ldots M_m = I.$$

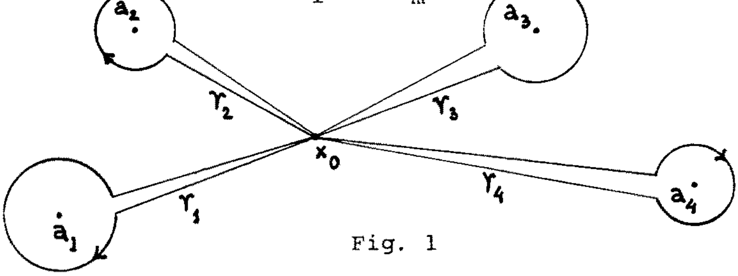

Fig. 1

The linear differential equation (7.1) for which all singularities are regular (i.e. all solutions of (7.1) have at most algebraic singularities everywhere) are called Fuchsian. To this class belong linear differential equations satisfied by algebraic functions. For Fuchsian equations monodromy groups and Galois groups are the same. For equations with irregular singularities, there are elements of a Galois group corresponding to Stokes multipliers, see §3.

From the algebraic point of view, an appropriate object is "an algebraic Galois (monodromy) group" of a linear differential equation defined as Zariski closure in $GL_n(\mathbb{C})$ of the Galois (monodromy) group $\mathfrak{M}$, i.e. the smallest algebraic group in $GL_n(\mathbb{C})$ which contains $\mathfrak{M}$.

Monodromy groups of linear differential equations were determined analytically only in a few cases, mostly for (generalized) hypergeometric equations and some other equations derived from them (cf. [29]). The problem of complutation of a monodromy group originates possibly with Fuchs, and we refer the reader to a review [30] on various numerical methods suggested at that time. Poincaré was the first who proposed to use multiple-integral representations of solutions of linear differential equations in order to expand elements of the monodromy group in series of polylogarithmic functions. The first effective solution of the direct monodromy problem along these lines belongs to Lappo-Danilevsky [31]. In his work Lappo-Danilevsky used polylogarithmic functions to solve matrix linear differential equations over $\mathbb{C}(x)$. E.g. let us consider an equation of the form

$$\frac{dY}{dx} = \Big(\sum_{i=1}^{m} \frac{A_i}{x - a_i}\Big)Y \tag{7.3}$$

(simple singularities at $a_1,\ldots,a_m$ for $n \times n$ matrices $A_1,\ldots,A_n$). A monodromy group of (7.3) with the normalization of solution $Y(x)$ by: $Y(x_0) = I_n$, is determined in terms of series in matrices A_i and in periods of polylogarithms as follows:

$$M_i = I + \sum_{j=1}^{\infty} \sum_{1 \le i_1 \le m,\ldots,1 \le i_j \le m} A_{i_1} \cdots A_{i_j} \times P_i(a_{i_1},\ldots,a_{i_j} | x_0). \tag{7.4}$$

Here periods of polylogarithmic functions are defined as:

$$P_i(a_{i_1},\ldots,a_{i_j} | x_0) = \int_{\gamma_i} \frac{L_{x_0}(a_{i_1},\ldots,a_{i_{j-1}} | x)dx}{x - a_{i_j}}$$

for a closed contour γ_i from x_0 travelling around a_i (and not containing any other a_i, within). The polylogarithmic functions are defined by induction:

$$L_{x_0}(a_{j_1},\ldots,a_{j_\nu} | x) = \int_{x_0}^{x} \frac{L_{x_0}(a_{j_1},\ldots,a_{j_{\nu-1}} | x)dx}{x - a_{j_\nu}}$$

where $L_{x_0}(a_{j_1} | x) = \log\frac{x-a_{j_1}}{x_0-a_{j_1}}$.

The series expansion (7.4) is convenient for analysis of singularities of monodromy matrices M_i as functions of coefficients A_i. However, a computer implementation of Lappo-Danilevsky-Poincaré expansions turned out to be unpractical for high (multiple) precision computations because of an excessive amount of matrix multiplications. In practice, the rate of convergence of series in (7.4) is very poor too.

Poincaré and Koch [24] proposed also a different method to compute invariants of a monodromy group of a linear differential equation using, essentially, Hill's method of determination of characteristic numbers of equations with irregular singularities. This method is much more practical for applications and allows some significant improvement using continued fraction expansions. We discuss some aspects of this method below in connection with the rank two second order linear differential equations.

The best results that we achieved so far use, as an algorithm, the very definition (7.2) of a monodromy group, and are based on the algorithm of the analytic continuation along the sides of a polygon described in §4. In practice, at each vertex the values of a solution (and its derivatives) were approximated by power series with the number of terms ranging from hundreds (25-50 digit accuracy) to thousands. The simplicity of the algorithms allow an easy implementation in FORTRAN, LISP or computer algebra systems.

Efficient solution of the direct monodromy problem can be used for the solution of the inverse monodromy problem if one of the Newton-like methods for solution of systems of nonlinear equations is applied. This approach to the inverse monodromy problem is particularly effective when the number of unknowns (accessory) parameters is a moderate one (see examples below for rank 2 equations). Otherwise methods based on the Riemann boundary value problem [32], particularly based on solutions of singular integral equations, are more appropriate. For Fuchsian equations satisfied by algebraic functions the solution to the inverse monodromy problem can be also used for solution of the inverse Galois problem.

Direct and inverse monodromy problems are very interesting in the multidimensional case. There the multiple-integral representation leads to a natural generalization of the Lappo-Danilevsky method; power series methods, though less efficient, are easier to implement. For the discussion of the multidimension Fuchsian equation see Deligne [33].

The Riemann existence theorem shows that any finite group G can be realized as a Galois group of a Riemann surface (an algebraic function field) over $\mathbb{C}(t)$ (even over $\bar{\mathbb{Q}}(t)$). The obstructions to the realization of G as a Galois group of a function field over $K(t)$ for an algebraic function field K were discovered by Hurwitz [34]. These obstructions are connected with possible automorphisms of Riemann surfaces, corresponding to a given set of generators of G that are realized as generators of a monodromy group of this Riemann surface. Hurwitz studies were considerably extended and generalized by Freid [35]. Later in works of Belyi [36] and Matzat [37] there appeared interesting "rigidity" property that guaranteed the realization of a finite group G as a Galois group over rational function field $K(t)$ for an Abelian algebraic number field K. Belyi's condition [36] is very simple: let G be generated by two elements a and b, $G = \langle a,b \rangle$ and let, whenever $G = \langle a',b' \rangle$ for $a' \sim a$, $b' \sim b$, $a'b \sim ab$, (sign $\sim$ means conjugation in G) there is (an inner) automorphism σ of G with $a^{\sigma} = a'$, $b^{\sigma} = b'$. Then G is "rigid".

This definition was generalized by Thompson [38] and Matzat [37], [39]. Their results allowed to prove the existence of Galois extensions over $\mathbb{Q}$ (sometimes over $\mathbb{Q}_{ab}$) of a large class of finite groups, including particularly many simple groups. Matzat et al. (see [39])were particularly successful in the proof of the existence of Galois extensions over $\mathbb{Q}(t)$ for 18 sporadic groups including M_{11}, M_{12} and J_1, J_2. On the other hand, Belyi [40] had shown the existence of Galois extensions over $\mathbb{Q}_{ab}$ of projective classical groups. Also Matzet et al. have shown that every transitive permutation group acting on ≤ 15 elements can be realized as a Galois group over $\mathbb{Q}(t)$.

We refer readers to [37-39] and [41] for the general definition of rigidity and proofs of the existence results.

These results are remarkable because they show that Riemann surfaces constructed (analytically) from the representation of generators of a given finite group are defined over a small number field, whenever these generators are chosen "rigidly". In principle, Matzat-Thompson results [37-39,41] indicate that one has only to construct Riemann surfaces with a given monodromy group,and this surface (after simple transformations, if necessary) will be defined over a small algebraic number field. There is only one problem with this constructive approach: it is not clear how in practice one constructs a Riemann surface with a given monodromy (Galois) group. The solutions to the inverse (analytic) Galois problem provides, consequently, an effective solution to the inverse arithmetic Galois problem. We hope to report elsewhere on our progress in implementation of the solution to the Riemann boundary value problem with applications to the solution of the inverse arithmetic Galois problem.

§8. Abelian Integrals and the Reduction Problem.

One of the classical problems of the early days of algebraic geometry was the reduction problem for Abelian integrals: to determine, when an Abelian integral (of the first, second or third kind) of genus g is reducible to (is expressed as) Abelian integrals of smaller genus. See [42], [43] for a summary of classical results. We will concentrate on two particular problems of reductions.

8.1: The first reduction problem is the problem of expression of Abelian integrals, particularly of elliptic integrals, in terms of elementary functions. This problem was formulated in the general case by Abel [15], who suggested different ways of its solution in the hyperelliptic case

$$\Gamma: y^2 = P_{2g+2}(x)$$

(for a polynomial $P_{2g+2}(x)$ of degree $2g + 2$ without multiple roots). Abel had shown that there exists a hyperelliptic integral on Γ:

$\int \frac{R_g(x)dx}{\sqrt{P_{2g+2}(x)}}$ reducible to the elementary functions if and only if

i) the divisor $(\infty^1) - (\infty^2)$ on infinity of Γ is of finite order; or, equivalently,

ii) the continued fraction expansion of $\sqrt{R_{2g+2}(x)}$ (at $x = \infty$) is periodic.

The feature i) is generalized to arbitrary Abelian integrals in the sense that the reducibility (to elementary functions) of arbitrary Abelian integrals is equivalent to the finiteness of the order of the divisor defined by an Abelian integral. The feature ii) was generalized in connection with the existence of periodic solutions of finite difference completely integrable equations of the Toda lattice $\ddot{x}_n = e^{x_{n+1}-x_n} - e^{x_n-x_{n-1}}$ type. Equivalently, the generalization of ii) to an arbitrary algebraic function field is expressed as a periodicity condition on a Hermite-Padé approximation to a basis of this function field, see [13].

Consequently, one has, in principle, an algebraic algorithm to determine an elementary expressability of an Abelian integral whenever the precise order of a given divisor on a Riemann surface can be determined. If this order is infinite, an Abelian integral corresponding to this divisor is a nonelementary function. If a bound on the order of a divisor can be obtained, the expression of an Abelian integral in terms of algebraic functions and their logarithms can be obtained in various ways. One of them should involve the construction of rational functions on a Riemann surface with a given divisor of zeroes and poles [44]. This approach naturally fits for implementarion in computer algebra systems, and became the proving grounds for testing the powers of new computer algebra systems. The first detailed analysis of the (first) reducibility problem in terms of computer algebra systems belongs to J. Davenport [44]. He considers particularly elliptic curves over $\mathbb{Q}$, where the torsion is bounded absolutely (due to Mazur's theorem), and so one has to check only a few cases of possible torsions. Recent progress in the development of algorithms for the reducibility problem belongs to B. Trager [45].

Practical implementation of any of these methods awaits a developed "Jacobian calculator" that would allow explicit calculations with divisors and rational functions on curves and their Jacobians.

The existing methods require a curve to be defined over $\bar{\mathbb{Q}}$. Then one can bound the possible torsions simply by looking on reductions of curves and their Jacobians modulo(good)primes. Moreover, even the computations to determine the precise order of the divisor in the Jacobian can be performed mod this(good)prime, which facilitates the speed of computations. The elliptic and hyperelliptic"calculators"(that are implemented) allow us to conduct these calculations for elliptic and genus two curves. See also Chebichef [76] for an explicit bound on the period of the continued fraction expansion of $\sqrt{R_4(x)}$ for $R_4(x) \in \mathbb{Z}[x]$.

Another algebraic algorithm arose from our work [46-47] on the Grothendieck conjecture on linear differential equations. (In passing we remark that one of the solutions of the problem of how to determine whether a second order differential equation has only algebraic solutions, requires the answer to the reducibility question, see [48].)

The Grothendieck conjecture asks whether a linear differential equation (over $\bar{\mathbb{Q}}(x)$) having sufficiently many (polynomial) solutions mod p for almost all p, has all its solutions as algebraic functions. We had proved this conjecture [46-47] for a large class of equations including Lamé equations, rank one equations over algebraic curves and other equations parametrized by meromorphic functions or arithmetic subgroups. Moreover, in all these cases, one can always find a finite set P of primes p that have to be checked only. This result has bearing on the reduction problem because Abelian integrals, if expressed by elementary functions, have by the Liouville theorem [42] the form

$$\int G(x,y)dx = w_0(x,y) + a_1 \log w_1(x,y) + \ldots + a_k \log w_k(x,y),$$

where $w_0(x,y)$ (an "algebraic" part) can be easily determined. Thus one has to determine the existence of sufficiently many solutions mod p of a linear differential equation satisfied by $\exp\{\int G(x,y)dx\}$ (etc.) for $p \in P$. This property, known as "p-curvature is equal to zero" [46] can be efficiently checked by looking at p^k-th coefficients at the expansion of $\exp\{\int G(x,y)dx\}$ for $p \in P$ and bounded k (usually $k = 1$ only). Thus the problem of "p-curvature zero" can be reduced to the examination of p-divisibility properties of coefficients of the expansion of the algebraic functions $G(x,y)$. The last problem is simply a problem of mod p computations of power series expansions of algebraic functions, and was one of the starting points in our work of §§2-3 on algorithms of power series expansions. The methods of §§2-3 (see particularly remarks concerning Atkin-Swinnerton-Dyer congruences) allow us to check very fast the necessary conditions of reducibility. The sufficient conditions take longer time to check, since known bounds on the size of P are obviously inflated (see [46]). One expects max P to be relatively small, but in the similar and related situation of Cheborateff's theorem (cf. [46], [49]) the best bounds on max P are achieved only assuming the Riemann hypothesis.

<u>8.2:</u> The second reducibility problem is even more geometric. It is a problem of reduction of Abelian integrals to a smaller genus. In its simplest form this is a problem of an expression of one (or g') of Abelian integrals of the first kind on a Riemann surface Γ of genus g in terms of integrals of the first kind on a Riemann surface Γ' of genus $g' < g$. Geometrically, it corresponds to the splitting of the Jacobian of Γ (up to the isogeny) into products of Jacobian of smaller dimensions. This geometric formalization is particularly interesting

in the case of reduction of Abelian integrals to elliptic ones. Particular cases of this problem are the following:

a) when a given Jacobian splits (up to isogeny) into product of g elliptic curves?

b) can one find for a given elliptic curves $E_1,\dots,E_g$ a curve of genus g whose Jacobian is isogeneous to $E_1 \times\dots\times E_g$?

A positive answer to b) is known only for $g \leq 3$ ($g = 2$ - Jacobi, see [43]; $g = 3$- Kowalewski [50]). There are several algorithms to deal with a). If curves are defined over $\mathbb{Q}$, one should look first at the Frobenius characteristic polynomials for $J(\Gamma)$ for good primes p. Also for $g = 2$ and small degrees D of isogeny there are even explicit equations on the moduli of hyperelliptic curves (Jacobi for $D = 2$ and Humbert in some other cases).

The best approach to either a) or b) lies, however, in the transcendental form, in the analysis of the Riemann period matrix of Γ. An appropriate criterion (Kowalewski-Painlevé) states [43], [50]: in order for g' Abelian integrals of the first kind $\int u_1,\dots,\int u_g$, of genus g (on Γ) to be reducible to the integrals of genus $g' < g$, it is necessary and sufficient for their $2gg'$ periods $\Omega_{i,j}$ ($i = 1,\dots,g'$; $j = 1,\dots,2g$) to be expressed in terms of $2g'g'$ numbers $\omega_{i,i'}$ ($i = 1,\dots,g'$; $i' = 1,\dots,2g'$) with (rational) integral coefficients:

$$\Omega_{i,j} = \sum_{i'=1}^{2g'} m_{j,i'}\cdot\omega_{i,i'} \quad (i = 1,\dots,g';\ j = 1,\dots,2g).$$

This criterion seems to be best suited to study the reduction problem. In the preceeding problem 8.1 of the <u>elementary reduction of Abelian integrals</u> this transcendental problem is equivalent to the question: whether all periods of the Abelian integral (say, $\int \frac{R(x)dx}{\sqrt{P(x)}}$) are rational multiples of $2\pi i$? (Here one takes $P(x)$, $R(x)$ with an appropriate norming.)

The solution to the reduction problem naturally brakes into two parts: a) to compute with a multiple ("infinite") precision periods of Abelian integrals, and b) to find $\mathbb{Z}$-relations between them. Problem b) is a familiar problem from multidimensional continued fractions, and there are several methods (a few of them quite new), how to find them. The solution of problem a) is given by our monodromy program, applied to Fuchsian linear differential equations satisfied by Abelian integrals of the first kind. The speed of computations is of order $O(M)$, where M is the precision of computations (see §4). In fact, the speed can be improved to $O((\log M)^{O(1)})$ if the transformation formulas for θ-functions are used.

The transcendental approach is particularly attractive, because often it allows us to find explicitly the mapping from Γ to Γ'. This is true, e.g. in the hyperelliptic case, when $g' = 1$ cf. [43].

The transcendental solution to the reduction problem was realized by us in the hyperelliptic case (arbitrary genus), and for hypergeometric curves $y^n = (x-a)^m \cdot (x-b)^k$, $y^n = (x-a)^m \cdot (x-b)^k \cdot (x-c)^\ell$.

The reduction problem, particularly, problem b) is of importance in a variety of situations. E.g. the factorization problem (see below) will run faster, if you use simultaneously g curves $E_1, \ldots, E_g$ and carry out the multiplication in $J(\Gamma)$ isogeneous to $E_1 \times \ldots \times E_g$, see [21,§6].

Another problem related to the reducibility: whether all solutions to the many particle problems

$$\ddot{x}_i = \sum_{j \neq i} \wp'(x_i - x_j): \quad i = 1, \ldots, n$$

(with $\wp(x)$ being a Weierstrass elliptic function) are expressed in terms of n elliptic functions. We know the positive answer for $n = 2$ and 3 only, see [51].

§9. Formal Completions of Abelian Varieties with Applications to Primality and Factorization Testing.

Our work on the Grothendieck conjecture in [49,47,46] led us to a better understanding of the connection between the analytic properties of Padé approximations to power series and the arithmetic properties of these power series (p-adic convergence for various p). This connection sheds light on the converse to the Eisenstein theorem, according to which power series expansions of algebraic functions have nearly integral coefficients. In [46] and [52] we proved for the first time a true converse to the Eisenstein theorem for the class of functions that can be uniformized by meromorphic functions in $\mathbb{C}^g$. The connection between archimedian analytic properties and the local ones was further exploited by us using methods of formal groups over $\mathbb{Z}$, $\mathbb{Z}_p$

and $\mathbb{F}_p$. The object of our primary interest were formal completions of Abelian varieties, in particular of elliptic curves over $\mathbb{Q}$ (see [27] for a review of formal groups in this case). Among the applications of our results [52] was partial but effective solution of the Tate conjecture on the bijectivity of the map $\mathrm{Hom}(A,B) \otimes \mathbb{Z}_\ell \mapsto \mathrm{Hom}(T_\ell(A),T_\ell(B))$ for Abelian varieties A and B over algebraic number fields. The Tate conjecture for elliptic curves was proved by Serre [53] for all cases but the one in which A and B have integral invariants but no complex multiplication. Faltings [54] proved (ineffectively) the finiteness of the isogeny classes for arbitrary Abelian varieties, solving the Tate, Schafarevich and Mordell conjectures. Applying our converse to the Eisenstein theorem [46,52] and Honda's [55] criterion of isogeny of formal groups over $\mathbb{F}_p$ we proved [52] the effective version of the Tate conjecture for all elliptic curves. For an elliptic curve $E/\mathbb{Q}$ with Weierstrass equation $y^2 = 4x^3 - g_2x - g_3 (g_2, g_3 \in \mathbb{Z})$ and the period lattice $\mathcal{L}$ we denote by $\Delta(E)$ the area of the fundamental parallelogram of $\mathcal{L}$ and $H(E) = \max(|g_2|^{1/4}, |g_3|^{1/6})$, so that $H(E) \le \gamma_1 \Delta(E)^{-2} \max(1, \log H(E))^{1/2}$.

Proposition 9.1: Let $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$ be elliptic curves defined over $\mathbb{Q}$. Then for every $\epsilon > 0$ there exists an effective constant $c_\epsilon > 0$ depending only on ϵ such that the following conditions are satisfied. If E_1 and E_2 have the same number of rational points (mod p) for any $p \le c_\epsilon \max\{1, \Delta(E_1)^{-1}\Delta(E_2)^{-1}\}^{1+\epsilon}$, then E_1 and E_2 are isogeneous over $\mathbb{Q}$ and, moreover, the degree of isogeny between E_1 and E_2 is bounded by $c_\epsilon \max\{1, \Delta(E_1)^{-1}\Delta(E_2)^{-1}\}^{1+\epsilon}$.

Our methods were also applied in [52,§3] to determine effectively all isomorphism classes of elliptic curves isogeneous to a given elliptic curve over $\bar{\mathbb{Q}}$. We have also an effective answer to the Tate conjecture for all Abelian varieties with real multiplications (generalization of Serre's and Ribet's results).

Interesting applications of formal groups of Abelian varieties mod p involve primality and factorization tests. All these tests generalize the famous primality (and factorization) tests based on Fermat's little theorem:

$$x^p \equiv x \pmod p$$

for any x (mod p).

However, instead of a multiplicative group one uses the action of a Frobenius automorphism $F_p: x \to x^p$ on a commutative algebraic group (Abelian variety).

A general version of a little Fermat theorem can look like this.

Fermat Theorem: Let an algebraic group A be defined over $\mathbf{F}_q$ (e.g. A is a reduction of an algebraic group scheme defined over $\mathbf{Z}[1/N]$ for $(N,P) = 1$), and let $P(x)$ be a characteristic polynomial of a Frobenius automorphism F_q of A. Then for an arbitrary X of A, the sequence of multiplies

$$X_m = m_*X \ (= [m]_A(X)): \quad m \in \mathbf{Z}$$

in the group law of A has a rank of apparition of p, and this rank $\tau(p)$, divides $P(1)$. I.e.

$$X_m = \bar{0} \quad \text{in} \quad A/\mathbf{F}_q$$

if and only if

$$\tau(p) \mid m$$

for $\tau(p) \mid P(1)$.

Similarly to classical p-1 and p+1 primality tests (including Lucas-Lehmer tests for primality of Mersenne numbers cf. [6]),the necessary primality test of the little Fermat's theorem can be made into a sufficient primality test by analyzing the precise order of X. These tests are practically efficient, because the computation of the characteristic polynomial of Frobenius F_p requires only polynomial (in log p) number of operations.

We had implemented a variety of elliptic primality tests that are particularly useful for various generalizations of Lucas-Lehmer sequences, i.e. for the testing of primality of solutions of second order linear recurrences, rather than first order recurrences as it used to be for numbers of the form $ab^n \pm 1$. However only a few numbers of this form are prime, and these are rare and require extensive sieving. We propose an elliptic generalization of Mersenne numbers arising from the so called elliptic divisibility sequences [56]. An elliptic divisibility sequence is defined typically as

$$\psi_n = \frac{\sigma(nu)}{\sigma(u)^{n^2}}$$

for the Weierstrass σ-function, and for a parameter u corresponding to a curve defined over $\mathbb{Z}$, and a rational point u on it. If an elliptic curve has, in addition, a complex multiplication in the quadratic field K, then one can define a new sequence

$$\psi_\mu = \frac{\theta(\mu u)}{\theta(u)^{\mathrm{Norm}(\mu)}}$$

for integers μ of K. Here the normalized θ-function corresponding to K is

$$\theta(u) = \sigma(u) \cdot e^{-\frac{1}{2} G_2 \cdot u^2}$$

for [57] $G_2 = \lim_{s \to 0+} \sum_{\substack{\omega \in \mathcal{L} \\ \omega \neq 0}} \omega^{-2} \cdot |\omega|^{-2s}$.

These sequences ψ_n and ψ_μ are divisibility sequences, because

$$\psi_\mu \text{ divides } \psi_\eta$$

whenever μ divides η.

Since ψ_μ grows as $e^{O(\mathrm{Norm}(\mu))}$, it takes much less sieving to find candidates ψ_p (or ψ_μ for $p = \mathrm{Norm}(\mu)$) for primality. Even for the simplest elliptic curves we found primes of this form having hundreds of digits.

Finally, factorization tests can be also constructed via the little Fermat theorem in a manner generalizing Pollard's p-1 and p+1 factorization tests. See the Wagstaff's lecture (this volume) on these and Lentra's algorithm. Roughly speaking this algorithm proceeds as follows. For a given composite n, one chooses a "random" elliptic curve $E \pmod{n}$ and a point X on it.

Then for an appropriate "seed" number $N = \ell\mathrm{cm}\{1,\ldots,M_n\}$ (with not too large M_n) one looks at $\gcd([N]_E(X),n)$. With a non-zero probability one recovers a nontrivial factor of n. Thus, to factor n this procedure has to be repeated.

A crucial point is the minimization of the number of operation in computation of the algebraic law of addition. These and other problems of speeding up the computations were analyzed by us some time ago using the SCRATCHPAD II system. These results are summarized in

[21]. E.g. we proposed in [21] to use in the factorization algorithm the cubic form $x^3 + y^3 + z^3 = Dxyz$ of the elliptic curve, for which the law of addition of two points is particularly efficient: $(x_1,y_1,z_1) \oplus (x_2,y_2,z_2) = (x_3,y_3,z_3)$, where

$$y_3 = x_1^2 y_2 z_2 - x_2^2 y_1 z_1,$$
$$x_3 = y_1^2 x_2 z_2 - y_2^2 x_1 z_1,$$
$$z_3 = z_1^2 y_2 x_2 - z_2^2 y_1 x_1,$$

(for $x_1 = x_2$, $y_1 = y_2$, $z_1 = z_2$, one puts $x_3 = y_1(z_1^3 - x_1^3)$, $y_3 = x_1(y_1^3 - z_1^3)$, $z_3 = z_1(x_1^3 - y_1^3)$).

Tests of algorithms were performed in summer of 1985 and showed excellent speed for primality proving for 100-300 digit numbers and factorization of 40-70 digit numbers on IBM mainframes.

§10. Formal Completions of Elliptic Curves and Characteristic Classes

Algebraic topology continues to be a proving ground for various methods of number theory and algebra (e.g. see Landweber's lecture in this folume). Recently new theories in cosmology led to a new look on classical problems of vanishing of characteristic classes.

Landweber and Stong were for some time studying the characteristic classes that completely characterize spin-manifolds with a nontrivial action of a circle group S^1. These studies are connected with Witten's problem on the index of Dirac operator associated with the tangent bundle for such manifolds. The (conjectural) description of characteristic classes is given in terms of formal groups connected with elliptic curves.

In our part of this work, computer algebra calculations turned out to be very useful. First of all we need a few definitions [58].

An important definition is that of a multiplicative sequence $\{K_j(p_1,\dots,p_j)\}$ of polynomials in $p_{j_1},\dots,p_{j_r}$ or weights $j = j_1+\dots+j_r$. These are sequences for which any power series identity $\Sigma p_i z^i = (\Sigma p_i' z^i)(\Sigma p_i'' z^i)$ implies the identity $\Sigma K_j(p)z^j = (\Sigma K_j(p')z^j)(\Sigma K_j(p'')z^j)$. The multiplicative sequence is completely determined by its characteristic series

$$P_K(x) = \Sigma_{n=0}^{\infty} \varphi_n(x,0,\ldots,0).$$

For a manifold M^{4n} we have a genus $\varphi([M^{4n}])$ associated with the series $P_K(x)$:

$$\varphi([M^{4n}]) = \varphi_n(p_1,\ldots,p_n)[M^{4n}]$$

where $p_i = p_i(M)$ are i-th Pontryagin classes of tangent fiber of M: $p_i \in H^{4i}(M)$.

Two of the most important genra are the signature $\tau(M)$--corresponding to the characteristic series $x/\tanh x$, and the $\hat{A}$-genus--corresponding to the series $x/(2\sinh(x/2))$.

Remark: The relationship between the formal groups and genra is the following. If $P(x)$ is a characteristic series, then for a power series $h(x)$ defined by $h(x) = x/P(x^2)$, its formal inverse is $h^{-1}(x) = \Sigma_{n=0}^{\infty} \frac{\varphi([\mathbb{CP}^{2n}])}{2n+1} x^{2n+1}$ the logarithm of the commutative one-dimensional group law $F(x,y) \overset{\text{def}}{=} h(h^{-1}(x) + h^{-1}(y))$.

According to Atiyah and Hirzebruch $\hat{A}$-genus vanishes on (closed and connected) Spin-manifold with a nontrivial action of S^1. If this action is also of odd type, then the signature vanishes too. The action of S^1 on M is odd, if $M^{S'} \neq \emptyset$ and the components of $M^{\mathbb{Z}_2}$ have codimensions $\equiv 2 \pmod 4$ with $\mathbb{Z}_2 = \{1,-1\} \subset S^1$.

Apparently, it is possible to describe all characteristic numbers vanishing on all Spin-manifolds with an odd S^1-action.

Landweber-Stong showed that for this it is enough to determine all characteristic classes that vanish on $[\mathbb{CP}(\xi^{2m})]$, $\xi^{2m} \to B$ being a complex vector bundle of even dimension over a compact oriented manifold. Landwever-Stong and Ochanine determined the ideal of all rational multipliers of bordism classes $[M]$ of Spin manifolds admitting smooth semi-free S^1-action of odd type. For this they used properties of formal groups associated with elliptic curves.

One looks at KO characteristic classes $\rho_k = \pi_k + \Sigma_{0<|\omega|<k} a_\omega^k s_\omega^\pi$ vanishing on all $\mathbb{CP}(\xi^{2m})$ and on the genus $\rho_t = \Sigma_{k\geq 0} \rho_k t^k$. Answering the problem of Landweber-Strong [59] we proved [60] that all coefficients a_ω^k are integers. The proof is based on the interpretation of a_ω^k as coefficients of elliptic modular forms.

From ρ_t one obtains a power series $f_t(y)$ (as a generating function of a multiplicative characteristic class ρ_t):

$$f_t(y) = 1 + yt + \sum_{k\geq 2} p_k(y)t^k,$$

$p_k(y) = \Sigma_{i=1}^{k-1} a^k_{(i)} y^i \in \mathbb{Q}[y]$ $(k \geq 2)$, with the (possible) normalization $a^k_{(1)} = 0$: $k \geq 2$.

In [59] $f_t(y)$ was determined from a certain nonlinear differential equation. We used computer algebra systems to derive a lower order differential equation on $f_t(y)$. We were able to determine $f_t(y)$ as a unique solution of this equation using the monodromy analysis. The coefficients of $f_t(y)$ are integral indeed and $f_t(y)$ turned out to be (of course!) a ratio of θ-functions. The final expressions are the following [60]:

$$f_t(y) = \prod_{n=1}^{\infty} \left\{\frac{1 - yq^{2n-1}/(1-q^{2n-1})^2}{1 - yq^{2n}/(1-q^{2n})^2}\right\}.$$

Here $t = -q + O(q^2)$ is defined as a q-series:

$$t = -\sum_{n=1}^{\infty} (2n+1)q^{2n+1}/(1-q^{2n+1}),$$

or, in classical notations:

$$t = \frac{1}{24}(1 - \vartheta_2(0)^4 - \vartheta_3(0)^4).$$

In particular, the coefficients of $f_t(y)$ are all integral.

§11. The Transcendence of Constants of Classical Analysis and Geometry and the Arithmetic Properties of Elements of the Monodromy Group.

One of the main problems of the transcendental number theory is to describe the arithmetic properties of constants of geometry and analysis, including the examination of their irrationality, transcendence and the establishment of measures of their diophantine approximations. Most of these classical constants are represented as integrals of elementary or algebraic functions over closed paths in a complex plane. These are various periods of algebraic varieties (e.g. periods of Abelian integrals), including values of Euler Γ- and B-functions at rational points. All these quantities appear as elements of the monodromy matrices of various linear differential equations "arising from geometry" [61], [46], [62]. We want to mention a few cases where some importance is attached to the transcendence problem of these quantities: the Grothendieck-Deligne conjecture on algebraic relations between periods of Abelian varieties (with complex multiplication) [63], [64], [65] and Milnor's conjecture on the linear independence of dilogarithms of the roots of unity. It is therefore crucial to gain the knowledge of the arithmetic properties of elements of the monodromy groups of linear differential equations with coefficients over $\bar{\mathbb{Q}}(x)$. Very little is known about the general properties of the monodromy groups, particularly from the point of view of algebracity or transcendence of their elements. To study the arithmetic properties of these numbers one has to develop good approximation methods that would allow us to study rational approximations to these numbers or their combinations. Short of reducing these numbers to the known transcendents, this is the only method how they can be studied in the transcendental number theory. This was, essentially, the starting point of our study of efficient and fast numerical methods to compute the analytic continuations of linear differential equations and the monodromy groups of these linear differential equations.

Unfortunately, not too much can be proved yet on the transcendence of elements of the monodromy group of an arbitrary linear differential equation over $\bar{\mathbb{Q}}(x)$. Moreover, it is even hard to speculate what kind of transcendence results one can expect. The relatively simple case is that of algebraic functions, where "the" monodromy group is always represented by matrices with algebraic entries. However, even in this case, as we already remarked (in §7 on inverse Galois problem) the relationships between degrees of the fields of moduli of the monodromy group and of the corresponding algebraic equation is far from obvious. If the monodromy group is not finite, we are led to the following crucial

Question 11.1: Let a linear differential equation be defined over $\bar{\mathbb{Q}}(x)$. When its monodromy group (or a Galois group for an equation with irregular singularities) has a representation by matrices with entries from $\bar{\mathbb{Q}}$?

If such a representation exists, we call a linear differential equation algebraically representable. It would be nice if the answer was: "if an equation over $\bar{\mathbb{Q}}(x)$ do not have algebraic function solutions, then it is not algebraically representable". This simplistic answer is incorrenct even if one puts additional constraints: a) an assumption that the equation be Fuchsian with rational exponents at regular singularities (the most interesting case for applications in geometry and analysis); b) that one should consider only those representations of the monodromy groups that correspond to the choice of the base point and the initial conditions for fundamental solutions being algebraic numbers.

Counterexamples to the simplistic answer, even with restrictions a) and b), are provided by the Gauss hypergeometric functions. Some of these functions have the monodromy group that is an algebraic subgroup of $GL_2(\bar{\mathbb{Q}})$; e.g. for classical modular functions it can be a congruence subgroup of $SL_2(\mathbb{Z})$. Nevertheless solutions are nonalgebraic. Moreover, a Fuchsian linear differential equation with 3 algebraic singularities and rational exponents at them generically has (some of) its monodromy group algebraically representable.

Inspired by these examples, one can ask, whether the algebraic representability is valid for all equations with the property a). The answer is an obvious "no", even for the first order linear differential equations satisfied by elliptic integrals. One then tries to find classes of Fuchsian equations, generalizing hypergeometric ones, that are algebraically representable. The second order equation with 4 singularities is the next class of equations. The most interesting among them are the equations uniformized by Fuchsian groups of Mobius transformations. These equations correspond, e.g. to the uniformization of punctured tori (whose modular invariant $k^2 = k^2(\tau)$ is the fourth singularity, together with $0,1,\infty$), or a Riemann sphere with 4 punctures at 0, 1, k^2 and ∞. For the punctured tori case the local exponents at $0,1$ and k^2 can be chosen as $(0,1/2)$ and at ∞ can be chosen as $(1/4,1/4)$. The fundamental arithmetic problem then is the determination of the arithmetic properties of the matrices of the Fuchsian group uniformizing these surfaces vs. the arithmetic properties of the coefficients of the Fuchsian equation with this group. This equation depends, apart from k^2, on a single constant, known as an "accessory parameter" [30], [66]. The transcendence problem we are facing is the following:

Problem 11.2: If one has a Fuchsian linear differential equation uniformizing a punctured tori with modular invariant k^2, so that the monodromy group of this equation is Fuchsian (of the first kind), is this group algebraically representable? Conversely, if one starts with a Fuchsian group of the first kind with two generators, and this group is algebraically representable, does the torus that this group uniformized yield an algebraic k^2? Is the corresponding accessory parameter algebraic?

An answer to Problem 11.2 is known so far only for 4 Fuchsian groups or 4 tori. In these cases the Fuchsian groups are congruence subgroups, and the corresponding differential equation arises as a lifting of a hypergeometric differential equation; see the discussion in [67] and references there, particularly to relationship with Apéry recurrences. See also Gutzwiller's lecture in this folume, where it is explained that these 4 groups are the only Fuchsian groups of their kind arising from the congruence subgroups.

It seemed to us, before we started our numerical experiments, that the Fuchsian uniformization is such a rigid condition that it would guarantee the algebraicity of the tori, parametrized by a Fuchsian subgroup of $SL_2(\bar{\mathbb{Q}})$. One of the major tests of our monodromy programs RIEMANN was the multiple precision computation of Fuchsian groups uniformizing a given torus (or a hyperelliptic Riemann surface) and tori uniformized by a Fuchsian group given by its two generators. These computations were checked against the possible appearance of algebraic numbers using the multidimensional generalizations of continued fractions. Our experiments did not discover any Fuchsian groups other the 4 congruence subgroups, generated by 2 matrices from $SL_2(\bar{\mathbb{Q}})$ that uniformize the tori with algebraic moduli k^2. Of course, we did not check all the possible groups; our main attention was concentrated on groups generated by matrices with algebraic integer entries. This unhappy conclusion seems to be valid for other Riemann surfaces uniformized by Fuchsian groups. The only exceptions that we know of, correspond to the lifting of the Schwartz's triangle functions and the lifting of the corresponding hypergeometric equations to linear differential equations uniformizing special Riemann surfaces.

Apart from numerical experiments, our knowledge of the arithmetic nature of the monodromy groups of linear differential equations is scarse even for orders 1 and 2. For Fuchsian equations of order 1 the problem is essentially equivalent to the study of periods of Abelian integrals of the first, second and third kind. The recent progress in the transcendence theory deals mainly with linear relations between these periods, and very little was added to the study of algebraic relations since [64]. For equations of the second order the transcendence theory can now treat only those equations that have all their solutions represented as uniform functions in the whole complete plane satisfying algebraic laws of addition. Geometrically this means that these linear differential equations describe the extension of an Abelian variety by a linear group. In all these cases it is relatively easy to prove the nonalgebraic representatability of the monodromy group of these equations at least under the condition b); this is more or less the consequence of the Schneider-Lang theorem [68]. What is now known even in these cases is the precise degree of transcendence of the field generated by the elements of the monodromy group of these equations.

Recently we were able to develop a new technique to study the transcendence of the elements of the monodromy group of an arbitrary linear differential equation over $\bar{\mathbb{Q}}(x)$. This method is based on a random walk in the upper half-plane and the uniformization of solutions of linear differential equations over $\bar{\mathbb{Q}}(x)$ by functions uniform in the upper half-plane [67]. To fit into the class of linear differential equations for which the transcendence results can be proved, linear differential equations should possess additional p-adic properties known as a global p-adic nilpotence for almost all p [61], [46], [62]. Instead of formulating this property, we give a different condition that, according to [62], guarantees that the equation is globally p-adically nilpotent for almost all p. This condition states that an equation has at least one G-function solution. A G-function $f(x)$ is a function regular at an algebraic point, say, $x = x_0$, and such that $f(x)$ has an expansion $f(x) = \Sigma_{N=0}^{\infty} c_N(x-x_0)^N$, where c_N are algebraic numbers and the sizes of c_N and the denominators of $\{c_0,\ldots,c_N\}$ grow not faster than a geometric progression in N [62]. E.g. all the Gauss hypergeometric functions ${}_2F_1(a,b;c;x)$ are G-functions at $x = 0$ for rational numbers a, b and c. We also will assume that a G-function solution of a given linear differential equation does not satisfy a linear differential equation over $\bar{\mathbb{Q}}(x)$ of lower order. Under these conditions the result is the following.

Theorem 11.3: If a linear differential equation over $\bar{\mathbb{Q}}(x)$ possesses a transcendental G-function solution as above, then a monodromy group of this equation with an algebraic base point and algebraic initial conditions of fundamental solutions at this point, is not algebraically representable provided that the base point is not a singular point of a linear differential equation.

The last condition is apparently crucial, as the example of the Legendre hypergeometric function ${}_2F_1(\frac{1}{2},\frac{1}{2};\frac{1}{2};x)$ ($=K(k)$ for $x = k^2$) shows. For the corresponding equation a monodromy group with the base point $x = 0$ and two initial branches $K(k)$ and $K'(k)$ is $\Gamma(2)$-the principal congruence subgroup of the modular group $SL_2(\mathbb{Z})$.

It is not clear whether the assumption of the existence of G-function solution is necessary.

§12. Rank Two Linear Differential Equations and Continued Fraction Expansions Associated with them.

Classical Gauss continued fraction expansions of a logarithmic derivative of a hypergeometric function correspond to rank one linear differential equations. These continued fraction expansions can be generalized to rank two linear differential equations, where the continued fraction expansions represent the elements of a monodromy group of a linear differential equation or elements of an extension of this group. These continued fraction expansions are often important in diophantine approximations. For example, particular kind of these continued fraction expansions for the Lamé equation with $n = -1/2$, that are globally nilpotent, describe Apéry's sequences of good rational approximations to $\zeta(2)$ and $\zeta(3)$ (see [61] for the p-adic differential equation part of it or [67]), we elaborate on this method below.

We remind that the rank of a linear differential equation at a given point is defined as the length of the recurrence determining the regular expansions of solutions at this point minus one. We prefer to look at singularities of a linear differential equation, where the rank is usually smaller than at regular points. One can assume here without loss of generality that this singularity is $x = 0$. Then the Frobenius method presented above shows that the most general form of the rank two differential equation of an arbitrary order is:

$$\sum_{i=0}^{n} P_{2,i}(x)x^i \frac{d^i}{dx^i} y = 0, \tag{12.1}$$

where $P_{2,i}(x)$ are quadratic polynomials: $i = 0,\ldots,n$. The (possible) singularities of (12.1) consist of 0, two roots of $P_{n,2}(x)$ and ∞. Let us denote these roots by α and β and let us assume that, say, $|\alpha| < |\beta|$. By a proper transformation $y' = y\cdot x^{\nu}\cdot(x-\alpha)^{\nu'}\cdot(x-\beta)^{\nu''}$, one can transform (12.1) into an equation, which has at each of singularities $x = 0, \alpha, \beta$ at least one local exponent zero. This means that there is a unique power series solution

$$y = \sum_{N=0}^{\infty} c_N x^N \tag{12.2}$$

of (12.1), regular at $x = 0$ and normalized by $c_0 = 1$. The coefficients c_N of (12.2) satisfy a three-term linear recurrence with coefficients polynomial in N. To exhibit this recurrence explicitly, we put:
$A_j(N) = P_{j,0} + P_{j,1}N + \ldots + P_{j,n}\cdot N(N-1)\cdots(N-n+1)$: $j = 0,1,2,$
where $P_{2,i}(x) = p_{2,i}x^2 + p_{1,i}x + p_{0,i}$: $i = 0,\ldots,n$. Then the recurrence satisfied by c_N is

$$A_2(N)c_N + A_1(N+1)c_{N+1} + A_0(N+2)c_{N+2} = 0 \tag{12.3}$$

(where we put $c_{-N} = 0$ for $N > 0$). The recurrence (12.3) can be used otherwise to determine the most general rank two linear differential equation with polynomial coefficients. Following Stiltijes method, one can associate with (12.3) a continued fraction expansion. This continued fraction expansion is connected with the asymptotics of solutions of the recurrence (12.3). According to Poincaré theorem, the asymptotics of solutions of (12.3) is determined by the roots of the asymptotic characteristic equation of (12.3) as $N \to \infty$: $p_{0,n}x^2 + p_{1,n}x + p_{2,n} = 0$. The roots of this equation are $1/\alpha$ and $1/\beta$. There are two linearly independent solutions of (12.3) with $N \geq 0$, which grow asymptotically as $|c_N| \sim 1/|\alpha|^N$ as $N \to \infty$. There exists a single (up to a multiplicative constant) solution $c_{\min,N}$ of (12.3) such that $|c_{\min,N}| \sim 1/|\beta|^N$ as $N \to \infty$. If $c_N^{(i)}$: $i = 1,2$ are two solutions of

(12.3) with the initial conditions, say, $c_0^{(1)} = 1$ (and $N \geq -1$) and $c_0^{(2)} = 0$, $c_1^{(2)} = 1$, then there are two constants C_1 and C_2 such that $c_{\min,N} = C_1 \cdot c_N^{(1)} + C_2 \cdot c_N^{(2)}$. The continued fraction expansion of $-C_1/C_2$ can be represented in terms of polynomials $A_i(N)$:

$$\frac{C_1}{C_2} = \ldots + \frac{A_0(N+1)/A_2(N-1)|}{|A_1(N+1)/A_2(N)} + \frac{A_0(N+2)/A_2(N)|}{|A_1(N+2)/A_2(N+1)} + \ldots .$$

One of the solutions, $c_N^{(1)}$, of (12.3) arises as coefficients in the power series expansion (12.2) of a solution of (12.1) regular at $x = 0$. Typically, the radius of convergence of $y(x)$ in (12.2) is $|\alpha|$, so that $C_2 \neq 0$. In this case one needs the second solution $c_N^{(2)}$ of the recurrence (12.3). Let us look to which differential equation the generating function of this solution,

$$(12.4) \qquad y_1(x) \stackrel{\text{def}}{=} \sum_{N\geq 0} c_N^{(2)} x^N,$$

corresponds. From the recurrence (12.3) it follows that the function $y(x)$ satisfies an nonhomogeneous linear differential equation associated with (12.1):

$$(12.5) \qquad \sum_{i=0}^{n} P_{i,2}(x) \frac{d^i y_1}{dx^i} = \text{const } (\neq 0).$$

The local multiplicities of solutions of (12.5) are the same as those of (12.1). This means that there are constants C_1 and C_2 (with a normalization $C_2 = 1$ according to the discussion above) such that $C_1 y(x) + C_2 y_1(x)$, analytically continued from $x = 0$ to $x = \alpha$, is regular at $x = \alpha$. Then the solution, $C_1 c_N^{(1)} + C_2 c_N^{(2)}$, is proportional to the minimal solution $c_{\min,N}$. As this discussion shows, the continued fraction expansion of $-C_1/C_2$ with elements being rational functions in N depends on the monodromy group of the equation (12.5) rather than that of (12.1). A nonhomogeneous equation (12.5) is, of course, equivalent to a homogeneous equation of order $n + 1$. This interpretation of continued fraction expansions with elements rational in N in terms of solutions of homogeneous and nonhomogeneous linear differential equations has interesting arithmetic applications to the study of irrationality and diophantine approximations of numbers having the form $-C_1/C_2$ under certain arithmetic conditions, see expositions in [69], [61]. In the arithmetic setting we assume that the equation (12.1) is globally nilpotent [62], [46], [61]. According to the main results of [62] this is equivalent to the condition that $y(x)$ in (12.2) is a G-function (see definitions in §11). In this case, according to [13], [62], $y_1(x)$ is also a G-function. This means that one has two sequences of rational numbers $c_N^{(1)}$, $c_N^{(2)}$ with denominators Δ_N ($\Delta_N \leq A^N$) such that $\max\{|c_N^{(1)}|,|c_N^{(2)}|\} << |\alpha|^{-N}$, but $|C_1 \cdot c_N^{(1)} + C_2 \cdot c_N^{(2)}| << |\beta|^{-N}$ and $|\beta| > |\alpha|$. Consequently,

$$\text{(12.6)} \qquad \frac{\Delta_N \cdot c_N^{(2)}}{\Delta_N \cdot c_N^{(1)}} = \frac{p_N}{q_N}$$

are sequences of rational approximations to $-C_1/C_2$. Under simple conditions on A, $|\alpha|,|\beta|$ (see e.g. Lemma 11.1 in [13]), one proves that $-C_1/C_2$ is irrational and, moreover, finds a bound for its measure of rational approximations. (For this one needs to assume only $\log|A| - \log|\beta| < 0$: the reason being a simple observation that a rational number cannot be too well approximated by rationals). Whenever an equation (12.1) arises from an integration of an algebraic function (e.g. hypergeometric functions with rational parameters) or a transformation of such an equation, the equation (12.1) is always globally nilpotent (Picard-Fuchs equations). In these cases c_N in (12.2) are, usually, integral. The Apéry recurrence furnishing sequences of rational approximations of the form (12.6) to $\zeta(2)$ and $\zeta(3)$ are particular cases of recurrences (12.3) corresponding to equations (12.1) that are liftings of hypergeometric equations [61], [67]. This method of investigation of the arithmetic nature of constants arising from monodromy groups of nonhomogeneous linear differential equations was generalized in [13] to equations of an arbitrary rank. In this method one generates an extension of a monodromy group of a linear differential equation that we describe. Let us start with an arbitrary linear differential equation

$$\text{(12.7)} \qquad \sum_{i=0}^{n} a_i(x) \frac{d^i y}{dx^i} = 0,$$

where $a_i(x)$ are polynomials: $i = 0,\ldots,n$. We assume that $x = 0$ is a regular singular point of (12.7), i.e. one can put $a_i(x) = x^i p_i(x)$: $i = 0,\ldots,n$ for $p_n(0) \neq 0$. Let r be the rank of (12.7) at $x = 0$,

$r = \max\{\deg p_i(x): i = 0,\dots,n\}$. In order to exclude a variety of trivial cases, we assume also that $x = 0$ is not an apparent singularity of any of the solutions of (12.7) and that at least one local multiplicity at $x = 0$ of (12.7) is zero. Then there exists a unique solution $y = y_1(x)$ of (12.7) regular at $x = 0$. In its expansion at $x = 0$

$$y_1(x) = \sum_{N=0}^{\infty} c_N x^N, \quad (\text{say } c_0 = 0)$$

the coefficients c_N satisfy a recurrence of length $r + 1$ with coefficients polynomial in N. If one looks at all r linearly independent solutions of this recurrence, one is lead to expansions at $x = 0$ of solutions of r nonhomogeneous linear differential equations associated with (12.7):

$$L[y] = x^{i-1}: i = 1,\dots,r-1, \tag{12.8}$$

where $L[y] \overset{\text{def}}{=} \Sigma_{i=0}^{n} a_i(x) \frac{d^i}{dx^i} y$ is a linear operator in the left side of (12.7). We put formally for $i = 0$ in (12.8), $L[y] = 0$. The system of equations (12.8) for $i = 0,\dots,r-1$ is equivalent to the single differential equation of order $n + r - 1$

$$\frac{d^{r-1}}{dx^{r-1}}(L[y]) = 0. \tag{12.9}$$

For $i = 1,\dots,r-1$ we consider solutions $y = y_{i+1}(x)$ of (12.8) regular at $x = 0$. Since local multiplicities of (12.8) are the same as that of (12.7), the spaces of such solutions of (12.8) are always one-dimensional and we can choose a normalized solution of the form

$$y_{i+1}(x) = \sum_{N=i}^{\infty} c_N^{(i+1)} x^N, \quad c_i^{(i+1)} = 1, \tag{12.10}$$

$i = 0,\dots,r-1$. Because the rank of the equation (12.7) at $x = 0$ is r exactly, any regular power series solution $y(x)$ of any of the equations $L[y] = q(x)$ for a polynomial $q(x)$, is a linear combination $y(x) = \Sigma_{i=1}^{r} C_i y_i(x) + q_1(x)$ for some constants $C_1,\dots,C_r$ and a polynomial $q_1(x)$. It also follows from (12.10) that all functions $y_1(x),\dots,y_r(x)$ are linear independent over $\mathbb{C}$. To construct a fundamental system of solutions of (12.9), let us denote by $Y_2,\dots,Y_n$ the $n-1$ solutions of (12.7) regular at $x = 0$ with local exponents corresponding to local exponents of (12.7) at $x = 0$ distinct from zero.

According to the Frobenius method, $Y_1 \overset{\text{def}}{=} y_1, Y_2, \ldots, Y_n$ is a fundamental system of solutions of (12.7). Since $x = 0$ is not an apparent singularity for any of the solutions of (12.7), the set of functions $\hat{Y} = (Y_1, \ldots, Y_n, y_2, \ldots, y_r)$ is a fundamental system of solutions of a linear differential equation (12.9) of order $n + r - 1$. Consequently we can study the monodromy group of a linear differential equation (12.9) (which we can call an extension of (12.7) at $x = 0$), by looking at the analytic continuation of the system $\hat{Y}$ of solutions. This particular monodromy group of (12.9) can be described as follows: let γ be a path in $\mathbb{CP}^1 \backslash S$ passing through $x = 0$, where S is the set of nonzero singularities of (12.7), and let us analytically continue the fundamental system $\hat{Y} = (Y_1, \ldots, Y_n, y_2, \ldots, y_r)$ along the path γ from $x = 0$. Then we have a linear transformation of this system of solutions:

$$\hat{Y} \underset{\gamma}{\rightarrow} \hat{Y} \cdot M_\gamma , \tag{12.11}$$

where M_γ is $(n+r-1) \times (n+r-1)$ matrix. It has a block form:

$$M_\gamma = \begin{pmatrix} A_\gamma & B_\gamma \\ C_\gamma & D_\gamma \end{pmatrix},$$

where A_γ is $n \times n$ matrix, B_γ is $n \times (r-1)$ matrix, etc. It is clear from (12.11) that in this block form A_γ is a monodromy matrix of (12.7) corresponding to γ and a fundamental system $Y_1, \ldots, Y_n$. Applying to (12.11) a linear operator $L[\cdot]$, we deduce that $(0, \ldots, 0, 1, \ldots, x^{r-2}) \underset{\gamma}{\mapsto} (0, \ldots, 0, 1, \ldots, x^{r-2}) \cdot M_\gamma$. Thus, $C_\gamma = 0$ and $D_\gamma = I_{r-1}$ is a unit $(r-1) \times (r-1)$ matrix. Consequently, M_γ has the following upper triangular block form

$$M_\gamma = \begin{pmatrix} A_\gamma & B_\gamma \\ 0 & I_{r-1} \end{pmatrix}.$$

We call the group generated by matrices M_γ an extension of a monodromy group of (12.7). The matrices B_γ, determining this extension, can be naturally interpreted from the point of view of (generalized) Hermite-Padé approximations associated with the linear recurrences of length $r + 1$ satisfied by coefficient $c_N^{(i+1)}$: $N \geq 0$. To interpret B_γ from the point of view of arithmetic applications, let γ_k be a path from $x = 0$ encircling a single nonzero singularity a_k of (12.7). Then we have

$$y_1 \underset{\gamma_k}{\longmapsto} \sum_{j=1}^{n} A_{i,j}^{(k)} Y_j,$$
$$y_{i+1} \underset{\gamma_k}{\longmapsto} \sum_{j=1}^{n} B_{i+1,j}^{(k)} Y_j + y_{i+1}: i = 1,\ldots,r-1.$$

For further analytis we assume that the equation (12.7) is Fuchsian. For example, we can assume that for finite singularities a_k of (12.7) one has $|a_1| <\ldots< |a_r|$. According to the Poincare theorem, the general solution of $r + 1$-order recurrence

$$\sum_{j=0}^{n} A_j(N+j)X_{N+j} \equiv 0: N \geq 0,$$

satisfied by $c_N^{(i)}$: $i = 1,\ldots,r$, has as the leading term of its asymptotics $\sim a_i^{-N}$ for an appropriate $i = 1,\ldots,r$. Consequently, we can make a linear transformation of the basis $\{y_1,\ldots,y_n\}$ of solutions (12.10) regular at $x = 0$ and obtain new functions:

$$\text{(12.12)} \qquad \bar{y}_1 \stackrel{\text{def}}{=} y_1, \text{ and } \bar{y}_{i+1} = \sum_{j=1}^{r} K_{ij} y_j: i = 1,\ldots,r-1$$

such that the functions $\bar{y}_1,\ldots,\bar{y}_{i+1}$ are regular at $x = 0$, $x = a_1,\ldots,x = a_i$ for $i = 1,\ldots,r-1$. For this new basis, the monodromy transformation rules (12.11) for the generators M_{γ_k} : $k = 1,\ldots,r$ have the form:

$$\text{(12.13)} \qquad \begin{gathered}(Y_1,\ldots,Y_n,\bar{y}_2,\ldots,\bar{y}_r) \underset{\gamma_k}{\longmapsto} (Y_1,\ldots,Y_n,\bar{y}_2,\ldots,\bar{y}_r)\cdot M_{\gamma_k}, \\ \bar{M}_{\gamma_k} = \begin{pmatrix} A_{\gamma_k} & \bar{B}_{\gamma_k} \\ 0 & I_{r-1} \end{pmatrix},\end{gathered}$$

where $(\bar{B}_{\gamma_k})_{j,i+1} = 0$ for all $j = 1,\ldots,n$ and $i = 1,\ldots,r-k$. E.g. $\bar{B}_{\gamma_1} = 0_{n\times(r-1)}$ etc. After the linear transformation (12.12) we normalize an extension of a monodromy group of (12.7) in the form (12.13) For general local multiplicities of (12.7) at $a_1,\ldots,a_k$, no further reduction in $\bar{B}_\gamma$ in $\bar{M}_\gamma$ in (12.13) is possible. While the invariants of the extension of monodromy group of (12.7) in the form (12.13) are essentially those of A_γ, the quantities in the transformations (12.12) can be interpreted as generalizations of the continued fraction expansions in the familiar form of Hermite-Padé approximations [70], [13]. We have already seen the continued fraction interpretation of the constant K_{11}/K_{12} from (12.12) in the case $r = 2$. Similar Padé approximation interpretation can be used in arithmetic applications to study the linear independence of numbers K_{ij} in (12.12) as we looked on the irrationality of K_{11}/K_{12} for $r = 2$. Nontrivial results can be obtained whenever the original equation (12.7) is globally nilpotent, e.g. whenever $y_1(x)$ is a G-function. The simplest case is, of course, that of y_1 being an algebraic function or its integral. An example of such situation had been studied in detail in [13, §6], when an equation (12.7) had the form

$$P_n y' + \frac{1}{2} P_n' y = 0, \qquad y_1(x) = 1/\sqrt{P_n(x)}$$

for a polynomial $P_n(x) = \prod_{i=1}^{n} (x - e_i)$ We proved there that for $P_n(x) \in \mathbf{Z}[x]$ and a PV-number root of $P_n(x)$, one obtains nontrivial measures of linear independence of periods of hyperelliptic integrals of the first and second kind for the surface $y^2 = P_n(x)$. Among the applications for $n = 3$ were measures of linear independence of $1, u, \zeta(u)$ for special algebraic values of $\wp(u)$, where $\wp'^2(u) = P_3(\wp(u))$. One can see also that the lifting of (generalized) hypergeometric equations to higher rank equations produces new examples of globally nilpotent equations where the values of (generalized) hypergeometric functions occur as numbers K_{ji} in (12.12).

We conclude this chapter with an example that shows that continued fraction expansions of C_1/C_2 are the generalizations of Gauss continued fraction expansions. For this we quote Pincherle's theorem proved in [80, §84]. According to this theorem we start with an arbitrary solution $y = y(x)$ of (12.1) such that $y(x) \cdot x^{-m+1}|_{x=\infty} = 0$ and $A_2(N) \cdot A_0(N) \neq 0$ for $N \geq m$. Then the ratio of two integrals of $y(x)$ has the following explicit continued fraction representation (cf. with (12.3))

$$A_2(m-1) \int_\gamma y(x) x^{-m} dx \Big/ \int_\gamma y(x) x^{-m-1} dx = - A_1(m) + \frac{A_2(m) A_0(m+1) |}{| A_2(m+1)} + \dots \tag{12.14}$$

The path γ of integration in (12.14) encompasses β. A very special case of the continued fraction expansion (12.14) in the case, when $n = 1$ and $y(x) = x^a (x-1)^b (x-t)^c$, is equivalent to one of the expressions of Gauss continued fraction expansion of two contiguous hypergeometric functions [80].

§13. Continued Fraction Expansions for Various Combinations of Elements of a Monodromy Group and Associated Three-term Linear Recurrences.

Though "explicit" expressions of elements of a monodromy group in terms of classical elementary transcendental functions are unknown, apart from a few special cases, one can try to express these quantities by other means. One of the examples of such an expression is the explicit form of Painlevé nonlinear differential equations, determing the isomonodromy deformation of a linear differential equation, as a function of regular singularities [19]. Another example,closer to our present discussion, is the continued fraction expansion of a logarithmic derivative of the Gauss hypergeometric function. In the latter example, the coefficients of the Gauss hypergeometric function satisfy a two-term linear recurrence and are represented in terms of binomial coefficients. However Gauss hypergeometric function itself does not, in general, have a simple rule of generation of continued fraction expansion. The logarithmic derivative of this function, or a ratio of any two contiguous Gauss hypergoemetric functions, has the continued fraction expansions with explicit expressions of its elements. A crucial property here is the existence of a three-term linear recurrence satisfied by three contiguous Gauss hypergeometric functions. Let us discuss how one can generalize this approach to functions satisfying Fuchsian second order linear differential equations with 4 regular singularities (Heun equations), among which the most interesting is the general Lamé equation [5] with an arbitrary rational n. The coefficients in a regular power series expansion of solution of Heun equation at a singularity satisfy three-term linear recurrences. Thus, one would expect the appearance of various continued fraction expansions in this setting; and we exhibit these continued fraction expansions that describe the ratios of various elements of a monodromy group of a Heun equation. Not all of ratios of elements of the monodromy group possess a continued fraction expansion. (E.g., it is not obvious how to obtain explicit continued fractions for the invariants of the monodromy group generated by the traces of products of the monodromy matrices.) However, for arbitrary elements of a monodromy group we show that there exists a uniform approximation by means of orthogonal polynomials in the accessory parameter. The new classes of explicit continued fractions expansions representing the ratios of elements of a monodromy group can be found for an arbitrary linear differential equation of rank two at singularities, and are generalizations of Gauss continued fraction expansions (see (12.14)). As for the remaining quantities of a monodromy group, that cannot be represented as explicit continued fraction expansions , one looks for an alternative simple expression. Expressions arising from analytic continuations are superior in numerical applications, but lack the conciseness. There are two other methods to obtain an analytic expression of a monodromy group of a linear differential equation. These are: the Poincaré-Lappo-Danilevsky method of expansion of a monodromy group in series of periods of polylogarithmic functions and the Koch infinite determinant method [24] (see §7). The Koch's method of infinite determinants is closely connected with the method of Hill's determinants [26], representing the characteristic numbers of solutions of equations with periodic coefficients. The relationship between the process of finding of Floquet exponents for equations with periodic coefficients and the determination of the invariants of the monodromy group was described in the classical literature, see particularly [5], [31], [71]. More recently this relationship was presented by Magnus [72] and Arscott (cf. [73]). Magnus [72] used the Fourier expansion of the elliptic functions to represent the invariants of the monodromy group of a Lamé equation in terms of Hill determinants. This method was used by L. Keen, H.E. Rauch and A. Γ. Vasques in their studies [74] of uniformization of punctured tori. These Hill determinants correspond to the infinite order recurrences depending on transcendental parameters $q = e^{2\pi i \tau}$, $K = K(k^2)$ and $E = E(k^2)$ of the fourth regular singularity $k^2 = k^2(\tau)$ of the Lamé equation. There are also more natural periodic expansions and three-term linear recurrences that lead to the expressions of the invariants of the monodromy group as ordinary three-diagonal Hill determinants depending algebraically on k^2 and an accessory parameter. These expressions are based on the Hermite-Ince-Darwin transformation (13.4) that reduces the Lamé equation to a trigonometric form (13.5). This form was used by Ince [75] to determine the periodic solutions of Lamé equation. Another new continued fraction expansion arises in connection with Hermite's third order linear differential equation, satisfied by products of solutions of the Lamé equation.

The most general Fuchsian second order linear differential equations with 4 regular singularities can be reduced by elementary transformations to the following Heun form:

$$\frac{d^2y}{dx^2} + \left(\frac{\gamma}{x} + \frac{\delta}{x-1} + \frac{\varepsilon}{x-a}\right)\frac{dy}{dx} + \frac{\alpha\beta x - q}{x(x-1)(x-a)}\,y = 0, \tag{13.1}$$

where $\alpha + \beta - \gamma - \delta - \varepsilon + 1 = 0$. Heun 's equation (13.1), unlike hypergeometric equation with 3 regular singularities, is not completely determined by its local exponents α, β, γ, δ, ε, but depends on the constant q-the accessory parameter. Let us denote by M_0, M_1, M_a three monodromy matrices of (13.1) corresponding to the monodromy transformations of any fixed system of fundamental solutions of (13.1), analytically continued along simple loops containing, respectively, 0, 1, a. These 3 matrices generate "a" monodromy group of (13.1), and Fricke's calculus of traces (cf. [66]) allows one to describe "the" monodromy group of (13.1) in terms of traces of products of these matrices. According to Fricke, 3 traces $\mathrm{Tr}(M_0M_1)$, $\mathrm{Tr}(M_0M_a)$, $\mathrm{Tr}(M_1M_a)$, in general, generate all invariants of the monodromy group of (13.1),and are known as Fricke parameters.

Among the Heun equations (13.1) one of the most interesting from the point of view of uniformization theory are Lamé equations for which $\alpha = \beta = \gamma = 1/2$ in (13.1). In analogy with elliptic modular forms, the forth singularity, a, is denoted by k^{-2}. If the local multiplicities of the Lamé equation at ∞ are $-n/2$ and $(n+1)/2$, then the algebraic form of the Lamé equation is the following:

$$\frac{d^2y}{dx^2} + \frac{1}{2}\left(\frac{1}{x} + \frac{1}{x-1} + \frac{1}{x-k^{-2}}\right)\frac{dy}{dx} + \frac{hk^{-2} - n(n+1)x}{4x(x-1)(x-k^{-2})}\,y = 0. \tag{13.2}$$

The transcendental Hermite's form of the Lamé equation (13.2) corresponds to the change of variables $x = (\mathrm{sn}(z,k))^2$, where $\mathrm{sn}(z,k)$ is the Jacobi sn-function. Under this transformation, one obtains from (13.2) [77]:

$$\frac{d^2y}{dx^2} + \{h - n(n+1)k^2\mathrm{sn}^2(z,k)\}y = 0. \tag{13.3}$$

There are also algebraico-transcendental forms of the Lamé equation corresponding to the Weierstrass parametrization of elliptic functions. The algebraic form is:

$$(13.2') \qquad \frac{d^2y}{dx^2} + \frac{1}{2}\left(\frac{1}{x-e_1} + \frac{1}{x-e_2} + \frac{1}{x-e_3}\right)\frac{dy}{dx} + \frac{H - n(n+1)x}{4(x-e_1)\dots(x-e_3)}y = 0$$

where we assume that $e_1 + e_2 + e_3 = 0$. The change of variables $\wp(u) = x$ reduces (13.2') to Halphen's form:

$$(13.3') \qquad \frac{d^2y}{du^2} + [H - n(n+1)\wp(u)]y = 0.$$

There exists a simple relationship between (13.3) and (13.3'): $z = iK' + u(e_1-e_3)^{1/2}$, $H = (e_1-e_3)h + n(n+1)e_3$, $k^2 = (e_2-e_3)/(e_1-e_3)$, where K and iK' are (quarter-periods) of Jacobi's elliptic functions. Transcendental forms (13.3) or (13.3') represent Lamé equations as second order linear differential equations with doubly periodic coefficients. This allows one to compute Fricke parameters of (13.2) in terms of the Floquet exponents of (13.2') by looking at the effects of shifts $z \to z + 2K$, $z \to z + 2iK'$, $z \to z + 2K + 2iK'$ on solutions of (13.2'). This method, based on the representation of Floquet's exponents in terms of infinite Hill determinants, was used in [72,74]. There is another representation of Lamé equation in terms of a second order linear differential equation with periodic coefficicnts. This is a representation of Lamé equation in trigonometric form indicated by Hermite and used by Ince [75]. Let us use Jacobi definitions of elliptic functions: $\varphi = \mathrm{am}(u,k)$ $(= \mathrm{am}\ u)$, if $u = \int_0^{\varphi}(1-k^2\sin^2 t)^{-1/2}dt$ $(= F(\varphi,k))$. Then $\mathrm{sn}(u,k) = \sin(\mathrm{am}\ u)$, $\mathrm{cn}(u,k) = \cos(\mathrm{am}\ u)$, $\mathrm{dn}(u,k) = (1 - k^2\sin^2(\mathrm{am}\ u))^{1/2}$. The substitution that transforms Lamé equation (13.3) to the trigometric form is the following:

$$(13.4) \qquad \mathrm{sn}(z,k) = \cos\zeta, \text{ where } \zeta = \pi/2 - \mathrm{am}\ z.$$

The substitution (13.4) transforms Lamé equation to

$$(13.5) \quad [1 - (k\cos\zeta)^2]\frac{d^2y}{d\zeta^2} + k^2\cos\zeta\sin\zeta\frac{dy}{d\zeta} + [h-n(n+1)(k\cos\zeta)^2]y = 0.$$

To find the Floquet exponent of the equation (13.5) with π-periodic coefficients, one looks at Fourier-type expansion of the solution of

(13.5): $y = \Sigma_{m=-\infty}^{\infty} c_m e^{(\mu i+2mi)\zeta}$. For solutions $y = y(x)$ of (13.2) it means the expansion: $y(x) = \Sigma_{r=-\infty}^{+\infty} c_r e^{(2r-\theta)iamz}$. The recurrence relations connecting the coefficients c_r are the following (cf. [75]):

$$(13.6)\quad \begin{aligned} &-\frac{k^2}{4}\{(\theta-2r)^2 - 3(\theta-2r) - (n+2)(n-1)\}c_{r+1} \\ &+ \{h' - (1-k^2/2)(\theta-2r)^2\}c_r - \frac{k^2}{4}\{(\theta-2r)^2+3(\theta-2r)-(n+2)(n-1)\}c_{r-1} \\ &= 0. \end{aligned}$$

Here we put $h' = h-n(n+1)k^2/2$. The recurrence (13.6) was studied in [75] for solutions of the Lamé equation (13.3) with periods 2K or 4K corresponding to $\theta = 0,1$, and conditions for $y = y(z)$ to be odd or even. The combination of these conditions leads to four possible classes of eigenvalues of Lamé equation, where h is a spectral parameter:

$y = Es^{2m+2}: y|_{z=0} = y|_{z=K} = 0 \quad : \quad h = a^{2m+2}$: period 2K,

$y = Es^{2m+1}: y'|_{z=0} = y|_{z=K} = 0 \quad : \quad h = a^{2m+1}$: period 4K,

$y = Ec^{2m+1}: y|_{z=0} = y'|_{z=K} = 0 \quad : \quad h = b^{2m+1}$: period 4K,

$y = Ec^{2m}: y'|_{z=0} = y'|_{z=K} = 0 \quad : \quad h = b^{2m}$: period 2K.

The trigonometric expansions of the eigenfunctions have the following form:

$$Ec^{2m} = A_0/2 + \sum_{r=1}^{\infty} A_{2r}\cos(2r\zeta), \quad Ec^{2m+1} = \sum_{r=0}^{\infty} A_{2r+1}\cos\{(2r+1)\zeta\},$$

$$Es^{2m} = \sum_{r=1}^{\infty} B_{2r}\sin(2r\zeta), \quad Es^{2m+1} = \sum_{r=0}^{\infty} B_{2r+1}\sin\{(2r+1)\zeta\}.$$

The recurrences on A_r, B_r follow from the general expression (13.6). We present these 4 recurrences in a different setting to generate two groups of orthogonal polynomials in the accessory parameter h. Let us put:

$$(13.7)\quad \begin{aligned} &\frac{1}{2}(n-2r)(n+2r+1)k^2X_r - [H-4(r+1)^2(2-k^2)]X_{r+1} \\ &\qquad + \frac{1}{2}(n-2r-3)(n+2r+4)k^2X_{r+2} = 0: \quad r = 1,\ldots; \\ &\frac{1}{2}(n-2r+1)(n+2r)k^2Y_r - [H-(2r+1)^2(2-k^2)]Y_{r+1} \\ &\qquad + \frac{1}{2}(n-2r-2)(n+2r+3)k^2Y_{r+2} = 0: \quad r = 1,\ldots, \ H = 2h'. \end{aligned}$$

Then the coefficients of Es^m, Ec^m give rise to solutions of (13.7) in the following way:

$$X_r = A_{2r},\ -HA_0 + (n-1)(n+2)k^2A_2 = 0;$$
$$X_r = B_{2r},\ -(H-8+4k^2)B_2 + \tfrac{1}{2}(n-3)(n+4)k^2B_4 = 0;$$
$$Y_r = A_{2r-1},\ -\{H-2+k^2 - n(n+1)k^2/2\}A_1 + \tfrac{1}{2}(n-2)(n+3)k^2A_3 = 0;$$
$$Y_r = B_{2r-1},\ -\{H-2+k^2 + n(n+1)k^2/2\}B_1 + \tfrac{1}{2}(n-2)(n+3)k^2B_3 = 0.$$

This implies that coefficients of Es^m, Ec^m give rise to two groups of orthogonal polynomials and two groups of polynomials adjoint to them. The uniform limits of these polynomials (as $r \to \infty$), after a proper normalization, tend to elements of the monodromy matrix M_0M_1 of the Lamé equation in its algebraic form (13.2). Let us assume here that $|k^2| < 1$. Then the fourth singularity a is $1 < |a|$, and the monodromy group of (13.2) is generated by 3 matrices: : M_0, M_1 and M_a corresponding to an arbitrary choice of two linearly independent solutions of (13.2). The invariants of the monodromy group of (13.2) are generated by 3 Fricke parameters: $x = \mathrm{tr}(M_0M_1)$, $y = \mathrm{tr}(M_0M_a)$, $z = \mathrm{tr}(M_1M_a)$. There exists a single algebraic relations connecting x,y,z. In the most interesting case of $n = -1/2$ (the punctured tori case) the relation is

$$x^2 + y^2 + z^2 = xyz. \tag{13.8}$$

We are interested in the determination of monodromy matrices M_0M_1, M_0M_a and M_1M_a and their traces. In fact, it is sufficient to determine M_0M_1, because other matrices can be identified with M_0M_1 if to apply the fractional transformations from the λ-group that send $\lambda = k^2 (= a^{-1})$ to 5 other values: $1 - \lambda$, $1/\lambda$, $1/(1-\lambda)$, $\lambda/(\lambda-1)$, $1-1/\lambda$, see [30] or [74]. There is a simple relationship between monodromy matrices of the Lamé equation in its algebraic form (13.2) and monodromy(Floquet) matrices of the transcendental form of the Lamé equation (13.3) Let $y_1 = y_1(z)$, $y_2 = y_2(z)$ be an arbitrary fundamental system of solutions of (13.3). Then, because $\mathrm{sn}^2 z$ has a period $2K$, $y_1(z+2K)$ and $y_2(z+2K)$ are solutions of (13.3) too. Thus:

$$\vec{y}(z+2K) = \vec{y}(z)\cdot T, \tag{13.9}$$

where $\vec{y}(z) = (y_1(z), y_2(z))^t$ and T is 2×2 monodromy (Floquet) matrix. One can identify T with M_0M_1. We choose as a fundamental system of solutions of (13.3) the following functions: y_s and y_c, $y_s|_{z=0} = 0$, $y_s'|_{z=0} = 1$; $y_c|_{z=0} = 1$, $y_c'|_{z=0} = 0$. Then the elements of the matrix T in (13.9),

$$T = \begin{pmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{pmatrix},$$

as functions of h, are related to the determination of eigenvalues a^m, b^m of (13.3). To see this, we note that the coefficient of (13.3) is even and periodic with period 2K. This allows us to express values of a fundamental system of solutions at 2K in terms of their values at K: $y_c(2K) = 2y_c(K)\cdot y_s'(K) - 1 = 1 + 2y_c'(K)y_s(K)$, $y_s(2K) = 2y_s(K)y_s'(K)$, $y_c'(2K) = 2y_c(K)y_c'(K)$, $y_s'(2K) = y_c(2K)$. Consequently, from (13.9) we deduce the following relationship between the values of y_c and y_s at $z = K$ and elements of T:

$$\begin{aligned} t_{11} &= 2y_c(K)y_s'(K) - 1 = 1 + 2y_c'(K)y_s(K), \\ t_{12} &= 2y_c(K)y_c'(K), \\ t_{21} &= 2y_s(K)y_s'(K), \qquad t_{22} = t_{11}. \end{aligned} \tag{13.10}$$

Also, according to the definitions of eigenvalues of the Lamé equation, the equations $y_s(K) = 0$, $y_c(K) = 0$, $y_s'(K) = 0$, $y_c'(K) = 0$ determine, respectively, the sequences of eigenvalues a^{2m+2}, a^{2m+1}, b^{2m+1}, b^{2m}. From this one can deduce that properly normalized sequences of polynomials

$$B_{2r}, B_{2r-1}, A_{2r-1}, A_{2r}$$

converge uniformly to, respectively:

$$y_s(K), y_c(K), y_s'(K), y_c'(K).$$

Since polynomials B_{2r} are adjoint to A_{2r}, and B_{2r-1} are adjoint to A_{2r-1}, the ratios $y_s(K)/y_c'(K)$ and $y_c(K)/y_s'(K)$ are approximated by rational fractions B_{2r}/A_{2r} and B_{2r-1}/A_{2r-1}, respectively, and have the explicit continued fraction expansions. Let us indicate explicitly the dependence A_i, B_i on accessory parameter h, we denote $A_i(h) = A_i$, $B_i(h) = B_i$. Then $A_i(h)$, $B_i(h)$ are polynomials in h and one has the uniform limits everywhere in h-plane:

$$(13.11)\qquad \begin{aligned} &\lim_{r\to\infty} B_{2r}(h)/\sqrt{r} \to \eta_{11}\cdot y_s(K),\\ &\lim_{r\to\infty} A_{2r}(h)/\sqrt{r} \to \eta_{22}\cdot y_c'(K),\\ &\lim_{r\to\infty} B_{2r-1}(h)/\sqrt{r} \to \eta_{12}\cdot y_c(K),\\ &\lim_{r\to\infty} A_{2r-1}(h)/\sqrt{r} \to \eta_{21}\cdot y_s'(K). \end{aligned}$$

Here η_{ij} are independent of h, $\eta_{ij} = \eta_{ij}(k^2,n)$ $(i,j = 1,2)$. The relations of the form (13.11) hold not only for expansion of solutions of Lamé equation, but in the general case for expansions of eigenfunctions of scalar linear differential equations with periodic coefficients, whenever Hill method can be applied. Such relations were presented explicitly for the first time in the case of Mathieu equation by Meixner [78]. The proof of (13.11) is similar to that of [78] for the Mathieu equation. It is based on the observation that the left and right sides of (13.11) are entire functions of h with the order of growth 1/2. These functions also have the same zeroes in the h-place, according to the discussion above.

In the cases: a) n-integer or b) $n = -1/2$ (the punctured tori case), the constants $\eta_{ij}(k^2,n)$ can be determined explicitly. In these cases the limit formulas (13.10)-(13.11) provide us with the uniform approximations of elements of the monodromy matrix T by algebraic combinations of explicit sequences of orthogonal polynomials $A_i(h)$ or $B_i(h)$. As we explained above, T can be identified with the monodromy matrix M_0M_1 of the Lamé equation in the algebraic form (13.2). The 4 sequences of polynomials give rise to two interesting explicit continued fraction expansion. These continued fraction expansions are

$$(13.12)\qquad \tau = \beta_0 - \cfrac{\alpha_0\gamma_0}{\beta_1 - \cfrac{\alpha_1\gamma_1}{\beta_2 - \cdots}}$$

for $\tau = y_s(K)/y_c'(K)$ and $\tau = y_c(K)/y_s'(K)$. The coefficients $\alpha_i,\beta_i,\gamma_i$ in (13.12) are rational functions of i, and are determined if one divides each of the recurrences (13.7) by $4r^2$ to obtain: $\gamma_{r+2}X_{r+2} + \beta_{r+1}X_{r+1} + \alpha_{r+1}X_r = 0$ (for $\tau = y_s(K)/y_c'(K)$) and $\gamma_{r+2}Y_{r+2} + \beta_{r+1}Y_{r+1} + \alpha_{r+1}Y_r = 0$ (for $\tau = y_c(K)/y_s'(K)$) cf. [75].

The uniform approximation of elements of monodromy matrices by sequences of orthogonal polynomials and the continued fraction expansions of certain ratios of these elements is typical not only for the Lamé equation, but for an arbitrary rank two linear differential equation, as reported above in §12. A particularly interesting example occurs when one considers a symmetric square of a Lamé equation. This third order linear differential equation is a rank 2 equation as well. This equation gives rise to a continuous fraction expansion which is not unlike the two continued fraction expansions in (13.12), but converges to the product of continued fraction expansions in (13.12)--to $y_c(K)y_c'(K)/(y_s(K)y_s'(K))$.

To describe the symmetric square of a second order linear differential equation, let us start with an arbitrary equation $d^2u/dx^2 + p(x)du/dx + q(x)u = 0$. Then all products $y = u_1u_2$ of the solutions u_1, u_2 of this equation satisfy a third order linear differential equation

$$d^3y/dx^3 + 3p(x)d^2y/dx^2 + [p'(x) + 4q(x) + 2p(x)^2]dy/dx + 2(q'(x) + 2p(x)q(x))y = 0.$$

This last equation is called a symmetric square of an equation satisfied by u. Hermite was the first (in his lectures of 1872-73) [77] to notice that a symmetric square of the Lamé equation (13.2) or (13.2') is a rank two equation again. This was used, in particular, to show that for a positive integer n, at least one product of solutions of Lamé equation is a polynomial. Later the same method was used by Lindemann (see [77]) for the Mathieu equation, where some product of two solutions is always an entire periodic function. For Lamé equation with an arbitrary n one can look at solutions of a symmetric square of a Lamé equation regular at two (neighboring) singularities. This determines an interesting feature similar to that discussed in §12, where we were looking at a linear combination of two solutions of a three-term linear recurrence, that converges fast to 0. It is precisely this linear combination, $a_n + \zeta(3)b_n \to 0$, of 2 solutions a_n, b_n of a three-term recurrence with integral b_n and "nearly integral" a_n, that was found by Apéry and was used to prove the irrationality of $\zeta(3)$. Here the function, $y(x) = \Sigma\, b_n x^n$ is determined from a solution of a symmetric square of the Lamé equation, [61]. In general, a symmetric square of the Lamé equation in the Weierstrass form (13.3') or (13.2') is

$$\text{(13.13')}\qquad \frac{d^3Y}{du^3} - 4(n(n+1)\wp(u)-H)\frac{dY}{du} - 2n(n+1)\wp'(u)Y = 0,$$

or

$$\text{(13.13")}\qquad P(x)\frac{d^3Y}{dx^3} + \frac{3}{2}P'(x)\frac{d^2Y}{dx^2} + \frac{1}{2}P''(x)\frac{dY}{dx} - 4(n(n+1)x-H)\frac{dY}{dx}-2n(n+1)Y = 0,$$

respectively, for $Y = y_1y_2$. Here y_1,y_2 are solutions of (13.2')-(13.3') and $P(x) = 4(x-e_1)(x-e_2)(x-e_3) = 4x^3 - g_2x - g_3$. The equation (13.13") has 4 singularities with exponents 0, 1/2, 1 at $x = e_i$ and with exponents $n + 1$, $1/2$, $-n$ at $x = \infty$. To apply the methods of §12 and to represent a certain ratio of elements of the connection (monodromy) matrix of (13.2')as an explicit continued fraction expansion, we start with two regular solutions of (13.2') with exponents 0 and 1/2 at $x = e_i$: $y_{1;i} = \Sigma_{N=0}^{\infty} c_{N;i}(x-e_i)^N$, $y_{2;i} = \Sigma_{N=0}^{\infty} c_{N;i}(x-e_i)^{N+1/2}$. Then $Y_1 = y_{1;i}^2$ and $Y_2 = y_{2;i}^2$ are two linearly independent solutions of (13.13") regular at $x = e_i$. The coefficients in the expansions of these solutions at $x = e_i$ satisfy the same three-term linear recurrence. This recurrence is

$$\text{(13.14)}\qquad \begin{aligned} &P'(e_i)r(r+1/2)(r+1)C_{r+1} + 4r((3r^2-n^2-n-3)e_i+H)C_r \\ &\quad + 2(r-n-1)(r+n)(2r-1)C_{r-1} = 0: \quad r \geq 1, \end{aligned}$$

where $Y = \Sigma_{r=0}^{\infty} C_r(x-e_i)^r$. Two linearly independent solutions of (13.14) are given by the expansions $Y_j = \Sigma_{r=0}^{\infty} C_r^{(j)}(x-e_i)^r$: $j = 1,2$. Let us assume, for simplicity, that $|e_i-e_j| < |e_i-e_k|$ for $\{i,j,k\} = \{1,2,3\}$. The roots of the asymptotic characteristic equation (13.14) as $r \to \infty$ are $1/(e_j-e_i)$ and $1/(e_k-e_i)$. Consequently there exists a unique (up to a multiplicative constant) solution $C_r^{(0)}$ of (13.14) such that $|C_r^{(0)}| \sim |e_k-e_i|^{-r}$ as $r \to \infty$. The solution $Y_0 = \Sigma_{r=0}^{\infty} C_r^{(0)}(x-e_i)^r$ of (13.13") is regular at $x = e_i$ and $x = e_j$, i.e. has the radius of convergence $|e_i-e_k|$, and is the linear combination of Y_1,Y_2: $Y_0 = A_1Y_1 + A_2Y_2$. Thus, as in §12, the ratio $\tau_0 = -A_2/A_1$ is represented by an explicit continued fraction expansion of the form (13.12), with elements $\alpha_i,\beta_i,\gamma_i$-rational functions of i deducible from the recurrence (13.14). Let us consider the connection formula between 2 fundamental systems of solutions at $x = e_i$ and $x = e_j$:

$$\text{(13.15)}\qquad (y_{1;i},y_{2;i}) = (y_{i;j},y_{2;j})\cdot M_{i,j},$$

for the connection matrix $M_{i,j} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

If we choose as a basis of solutions of (13.2') $\vec{y} = (y_{1;i}, y_{2;i})$, then the monodromy matrix M_α of (13.2') corresponding to the paths γ_α encompassing e_α can be expressed in terms of the connection matrix: $M_i = \mathrm{diag}(1,-1)$; $M_j = M^{-1}_{i,j} \cdot M_i \cdot M_{i,j}$. Under an appropriate normalization of $\vec{y}$ (when ad - be = 1), we have

$$M_j = \begin{pmatrix} ad + bc & ; & -2ab \\ -2cd & ; & -ad - bc \end{pmatrix}.$$

Since $Y_1 = y^2_{1;i}$, $Y_2 = y^2_{2;i}$, we have the following identification of τ_0:

(13.16) $$\tau_0 = ac/bd.$$

Simple linear transformations reducing (13.2') to (13.2) allow us to identify (in the case $|k^2| < 1$), M_i and M_j of (13.2') with the monodromy matrices M_0 and M_1 of (13.2). This identification and (13.15) allows us to identify the expression τ_0 in (13.16) with

$$\frac{y_c(K)y_c'(K)}{y_s(K)y_s'(K)} .$$

The explicit expression of the continued fraction expansion of this quantity follow directly from that of τ_0, i.e. from the recurrence (13.14). Consequently, not only $y_c/y_s'|_{z=k}$ and $y_c'/y_s|_{z=k}$ have explicit continued fraction expansions, but their product too. This property allows us to study the arithmetic nature of quadratic relations between certain constants of classical analysis in addition to linear relations, as in §12. Our arguments can be extended to higher order symmetric powers of linear differential equation of ranks 1, 2 or higher.

Continued fraction expansions of τ in (13.12) or τ_0, (13.16), do not allow us to express the invariants of the monodromy group--the Fricke parameter. We remark that the computation of h using the polynomial approximations (13.10)-(13.11) is inefficient due to slow convergence. This convergence can be somewhat sped up using different acceleration techniques (cf. references in [78]). If one wants to determine periodic solutions of Lamé equations, then the continued fraction representation (13.12) is clearly a superior method (see [75]). In the theory of Teichmuller spaces of punctured tori, periodic solutions of Lamé equation with $n = -1/2$ correspond to real points on the boundary of Teichmuller spaces in problems of simultaneous uniformization of two punctured tori. In general, for solution of uniformization problem we use numeric solution of the direct monodromy problem based on the power series method of §§3-4. Cf. this with the Hill determinant method of [77] applied in [74]. The uniformization problem of punctured tori with a given invariant k^2 is equivalent to the problem of determination of the value of the accessory parameter h in (13.2) or (13.3) such that the Fricke parameters x,y,z in (13.8) of the monodromy group of (13.2) are all real. The reality of x,y,z means that "the" monodromy group of (13.2) is a Fuchsian group. (See Gutzwiller, this volume, for the description of the fundamental domain of a punctured tori uniformized by a Fuchsian group.) Recent interest in the accessory parameter solution to the uniformization problem arose after Polyakov-Zamolodchikov work on conformally invariant field theories. Using the theory of Liouville equation, Takhatadjan and Zograf established a representation of the Weyl metrics on Teichmuller spaces in terms of explicit functions of accessory parameters furnishing the Fuchsian uniformation (see in [79]). To establish the connection with [79] we note that the problems of uniformization of punctured tori and of uniformization of a Riemann sphere with 4 punctures are equivalent. The uniformization problem for a Riemann sphere with 4 punctures at $0,1,a,\infty$ is equivalent to the determination of an accessory parameter in (13.1) with $\alpha = \beta = \gamma = \delta = \epsilon = 1$, for which the monodromy group of (13.1) is Fuchsian. The equations (13.1) with $\alpha = \beta = \gamma = \delta = \epsilon = 1$ are reducible to the Lamé form with $n = -1/2$ using a Halphen transformation [77]. This transformation is easier to describe for Lamé equation in the form (13.2'), with $P(x) = 4(x-e_1)(x-e_2)(x-e_3)$, where the Halphen transformation is: $x = \wp(u)$, $Y = y/\sqrt{\wp(u/2)}$ and $X = \wp(u/2)$. Then the transformed equation (13.2') is

$$P(X)\,\frac{d^2Y}{dX^2} + P'(X)\cdot\frac{dY}{dX} + 4(X + H)Y = 0,$$

i.e. (13.1) with $\alpha = \ldots = \epsilon = 1$.

According to [79] the Weyl metric for the Teichmuller space of a Riemann sphere with 4 punctures at $0,1,a,\infty$ has in the a-coordinate representation the form $m(a,a^*)da\,da^*$, where $m(a,a^*) = 1/2\pi\ \partial_{a^*}(S)$,

$S = (1/2-m)/(a(a-1))$. On Fig. 2 and Fig.3 one can see landscapes of $h = h(a)$ and of $m = m(a,a^*)$, respectively, in the a-complex plane obtained on a VAX780 after a few hours of computation of Fuchsian accessory parameters and numerical differentiation. The size of the grid is 51×51; computations were in double complex precision. This landscape incorporates the evaluation of about 3.10^7 terms of various power series expansions.

Numerical solution of the uniformization problem using the classical accessory parameter approach extends beyond the punctured tori situation to Riemann surfaces (see the Abelian varieties calculator, §1.5)). The key element in this approach is the fast computation of monodromy groups of linear differential equations using analytic continuation methods of §4. One can apply these methods to the uniformization of hyperelliptic surfaces of genus g, $g \leq 10$ or arbitrary Riemann surfaces of genus $g \leq 4$ on standard hardware even in FORTRAN. We are going to report on results of this work in next seminar.

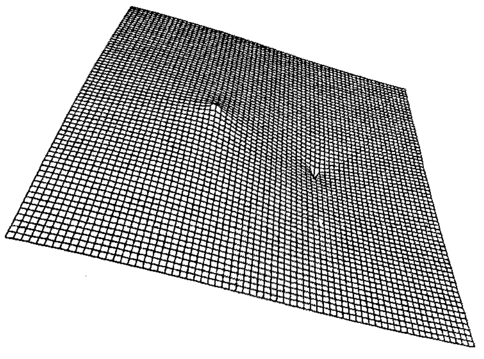

Fig. 2

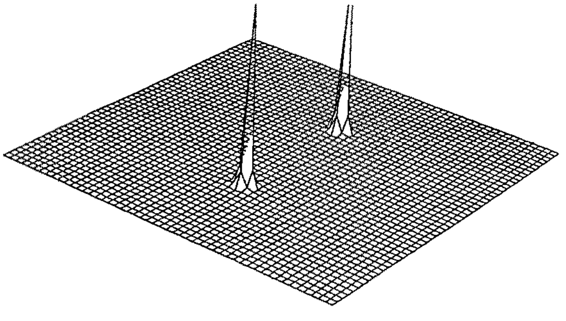

Fig. 3

References

[1] L. Fuchs, Gesammelte Mathematische Werke, bd 1-3, Berlin, 1900-1906.

[2] A. R. Forsyth, Theory of differential equations, v. I-VI, Dover reprint, 1959.

[3] F.G. Frobenius, Gesammelte Abhandlungen, Springer, N.Y., 1968, Bd. 1.

[4] H.T. Kung, J.F. Traub, All algebraic functions can be computed fast, J. Assoc. Comp. Mech. 25 (1978), 245-260.

[5] I.L. Ince, Ordinary differential equations, Dover, 1959.

[6] D.E. Kunth, The Art of Computer Programming, v. 2, 2nd ed., Addison-Wesley, 1981.

[7] J. Della Dora, E. Tournier, Formal Solutions of Differential Equations in the Neighborhood of Singular Points, in SYMSAC' 81 Proceedings (ed. P.S. Wang), Assoc. Computer Machinery, 1981, pp. 25-30.

[8] D.B. Chudnovsky, G.V. Chudnovsky, On expansion of algebraic functions in power and Puiseux series, IBM Research Report, RC11365, 9/13/85, 96 pp.

[9] R.P. Brent, H.T. Kung, Fast algorithms for manipulating formal power series, J. Assoc. Comp. Machinery, 25 (1978), 581-595.

[10] E. Hille, Ordinary differential equations in the complex domain, Wiley, N.Y., 1976.

[11] B.C. Carlson, Special Functions of Applied Mathematics, Academic Press, N.Y., 1977.

[12] R.P. Brent, Multiple-precision zero-finding method and the complexity of elementary function evaluation, in Analytic Computational Complexity (ed. by J.F. Traub), Academic Press, 1976, pp. 151-176.

[13] 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.

[14] D.V. Chudnovsky, G.V. Chudnovsky, Padé approximations to solutions of linear differential equations and applications to diophantine analysis, ibid., 85-167.

[15] N.H. Abel, Sur l'intégration de la formule différentielle $\rho \cdot dx/\sqrt{R}$, R and ρ étant des fonctions entières, J. Reine Angew, Math., 1 (1826), 185-221, = Oeuvres, v. 1, 104-144.

[16] F.G. Frobenius, L. Stickelberger, Über die addition und multiplication der elliptischen functionen, ibid., 88 (1880), 146-184.

[17] H.F. Baker, Note on the foregoing paper "Commutative differential operators", by J.L. Burchnall and J.W. Chaundy, Proc. Roy. Soc. London, A., 118 (1928), 584-593.

[18] G.V. Chudnovsky, Padé approximations and the Riemann monodromy problems, in Bifurcation Phenomena in Mathematical Physics, D. Reidel Publishing Company, Boston, 1980, 448-510.

[19] D.V. Chudnovsky, Riemann monodromy problem, isomonodromy deformation equations and completely integrable systems, ibid., 385-447.

[20] R.T. Baumel, J.L. Gammel, J. Nuttall, Asymptotic form of Hermite-Padé polynomials, IMA Journal of Appl. Math., 27 (1981), 335-357.

[21] D.V. Chudnovsky, G.V. Chudnovsky, Sequences of numbers generated by addition in formal groups and new primality and factorization test, IBM Research Report, RC 11262, 7/12/85, 1985, 102 pp., Advances in Applied Mathematics, 1986 (to appear).

[22] G. Andrews, Physics, Ramanujan and SCRATCHPAD, in Proceedings of the conference "Computer Algebra as a Tool of Research in Mathematics and Physics" (to appear).

[23] Parallel Processing Systems (ed. by D. Evans), Cambridge Univ. Press, 1982.

[24] H. vonKoch, Un théorem sur les intégrales irrégulieres des equations differentielles linéaires et scn application du problème de l'integration, Ark. för Math., 13 (1918), No. 15, 1-18.

[25] F.W.J. Olver, Asymptotics and Special Functions, Academic Press, 1974.

[26] H. Poincaré, Sur le déterminant de Hill, Bull. Astron., 17 (1900), 134-143 = Oeuvres, v. 8, 383-393, Paris, 1952.

[27] M. Hazewinkel, Formal Groups and Applications, Academic Press, 1978.

[28] E.R. Kolchin, Differential Algebra and Algebraic Groups, Academic Press, N.Y., 1973.

[29] B. Riemann, Oeuvres Mathématiques, Blanchard, Paris, 1966, 353-363.

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

[31] J.A. Lappo-Danilevsky, Mémoires sur la Théorie des Systèmes des Équations Différentielles Linéaires, Chelsea, 1953.

[32] The Riemann Problem, Complete Integrability and Arithmetic Applications, ed. by D.V. and G.V. Chudnovsky, Lecture Notes in Math., v. 925, Springer, N.Y., 1982.

[33] P. Deligne, Equations Differentielles à Point Singulier Reguliers, Lecture Notes in Math., v. 163, Springer, N.Y., 1970.

[34] A. Hurwitz, Über Riemannshe flachen mit gegeben verzweigungspunten, Math. Ann., 39 (1891), 1-61.

[35] M. Fried, Fields of definition of function fields and Hurwitz families. Groups as Galois groups, Comm. Algebra, 5(1977), 17-82.

[36] G.V. Belyi, On Galois extensions of a maximal cyclotomic field, field., Math. USSR Izvestija 14 (1980), 247-256.

[37] B.N. Matzat, Konstruktion von zahl-and funktionen-körpern mit vorgegebener Galoisgruppe, J. Reine Angew. Math., 349 (1984), 179-220.

[38] J.G. Thompson, Some finite groups which appear as Gal(L/K), where $K \leq \mathbb{Q}(\mu_n)$, J. Algebra, 89 (1984), 437-499.

[39] B.H. Matzat, Zum einbettungsproblem der algebraischen zahlentheorie mit nicht abelschem kern, Invent Math., 80 (1985), 365-374.

[40] G.V. Belyi, On extensions of the maximal cyclotomic field having a given classical Galois group, J. Reine Angew, Math., 341(1983), 147-156.

[41] Proceedings of the Rutgers Group Theory Year, 1983-84 (Ed. by M. Aschbacher, D. Gorenstein, R. Lyons, M. O'Nan, C. Sims, W. Feit), Cambridge Univ. Press, 1984.

[42] N.G. Chebotareff, Theory of Algebraic Functions, Gostechizdat, 1968 (Russian).

[43] H.F. Baker, Abel's Theorem and the Allied Theory Including The Theory of Theta Functions, Cambridge, 1897.

[44] J.H. Davenport, On the Integration of Algebraic Functions, Lecture Notes Computer Sci. v. 102, Springer, N.Y. 1981.

[45] B. M. Trager, Integration of Algebraic Functions, Ph.D. Thesis, M.I.T. 1984.

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

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

[48] F. Baldassarri, B.M. Dwork, On second order linear differential equations with algebraic solutions, Amer. J. Math. 101 (1970), 42-76.

[49] D.V. Chudnovsky, G.V. Chudnovsky, p-adic properties of linear differential equations and Abelian integrals, IBM Research Report RC10645, 7/26/84.

[50] S.V. Kowalewski , Über die reduction einer bestimintea classe Abel'schen integrale 3-en ranges auf elliptische integrale, Acta Math., 4 (1884), 393-414.

[51] D.V. Chudnovsky, Meromorphic solutions of nonlinear partial differential equations and many particle completely integrable systems, J. Math. Phys., 20 (1970), 2416-2422.

[52] D.V. Chudnovsky, G.V. Chudnovsky, Padé approximations and diophantine geometry, Proc. Natl. Acad. Sci. U.S.A. 82 (1985), 2212-2216.

[53] J-P. Serre, Quelques applications du théoreme de densité de Chebotarev, IHES Publ. Math., 54 (1981), 323-401.

[54] G. Faltings, Endlichkeitssätze für abelsche varietäten über zahlkörpern, Inv. Math., 73 (1983), 349-366.

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

[56] M. Ward, Memoir on elliptic divisibility sequences, Amer. J. Math., 70 (1948), 31-74.

[57] S. Lichtenbaum, On p-adic L-functions associated to elliptic curves, Inv. Math., 56 (1980), 19-55.

[58] F. Hirzebruch, Topological Methods in Algebraic Geometry, Springer, 1966.

[59] P.S. Landweber, R.E. Stong, Circle actions on spin manifolds and characteristic numbers (to appear).

[60] D.V. Chudnovsky, G.V. Chudnovsky, Elliptic modular functions and elliptic genera (to appear).

[61] B. Dwork, Arithmetic theory of differential equations, Symposia Mathematica, v. 24, Academic Press, N.Y., 1981, 225-243.

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

[63] G. Shimura, On some problems of algebraicity, Proceeding Intern. Congress of Math., Helsinki, 1978, v. 1, 373-379.

[64] G. V Chudnovsky, Algebraic independence of values of exponential and elliptic functions, ibid., 339-355.

[65] P. Deligne, Valeurs de fonctions L et périodes d'intégrales, Proc. Symp. Pure Math., v. 33, part 2, AMS, 1979, 313-346.

[66] R. Fricke, F. Klein, Vorlesungen über die theorie der automorphen functionen, 2v., Teubner, 1926.

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

[68] S. Lang, Introduction to transcendental numbers, Addison-Wesley, 1966.

[69] G.V. Chudnovsky, Explicit construction of auxiliary functions for transcendental numbers, Lecture Notes Math., v. 751, Springer, N.Y. 1979, 45-69.

[70] H. Padé, Oeuvres, Blanchard, Paris, 1984.

[71] N.P. Erugin, Lappo-Danilevsky method in the Theory of Differential Equations, Leningrad Univ. Press, 1956.

[72] W. Magnus, Monodromy groups and Hill's equation, Comm. Pure Appl. Math., 29 (1976), 701-716.

[73] F. M. Arscott, Periodic Differential Equations, Macmillan, N.Y., 1964.

[74] L. Keen, H.E. Rauch, A.T. Vasques, Moduli of punctured tori and the accessory parameter of Lamé's equations, Bull. Amer. Math. Soc., 255 (1979), 201-230.

[75] J.L. Ince, Periodic Lamé functions, Proc. Edinb. Math. Soc., 41 (1923), 94-100 and 60 (1939), 47-63.

[76] P.L. Chebichef, Sur l'integration de la différentielle $(x+A)dx/\sqrt{x^4+ax^3+bx^2+cx+d}$, Bull. Acad. Impériale de Saint-Pétersbourg, 3 (1861), 1-12.

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

[78] J. Meixner, Orthogonal polynomials in the theory of Mathieu functions, I, II, Arch. Math. 36 (1981), 162-167; 39 (1982), 46-50.

[79] L.A. Takhtadjan, P.G. Zograf, The Liouville equation action-the generating function for accessory parameters, Funct. Anal., 19 (1985), 67-68.

[80] O. Perron, Die Lehre von den Kettenbrüchen, Teubner, 1929.