COMPUTING ARITHMETIC PICARD-FUCHS EQUATIONS

JEROEN SIJSLING

These are the extended notes for a talk given at the Fields Institute on August 24th, 2011, about my thesis work with Frits Beukers at the Universiteit Utrecht. The style of these notes is rather rough, I am afraid; it is certainly not in the good Theorem-Proof tradition. However, I need to paint with a broad brush in order not to get bogged down into technical details that are of minor interest to geometers. There is a very useful general introduction to Shimura curves and the associated groups in the notes at `http://jmilne.org/math/xnotes/svi.html`.

1. Fuchsian equations from geometry

We consider second-order Fuchsian differential equations. The equations living on the curve $\mathbb{P}^1_{\mathbb{C}}$ with three singularities are well-understood: putting the singularities at $\{0, 1, \infty\}$, these are the *hypergeometric equations*

$$(z(z-1)\frac{d^2}{dz^2} + ((a+b+1)z - c)\frac{d}{dz} + ab)u = 0. \tag{1.1}$$

Here a, b, c are arbitrary parameters. These equations have been studied extensively; their history starts with Schwarz and continues into modern generalizations due to Gel'fand-Kapranov-Zemlinsky also studied by Beukers, Bod, and Heckman.

The equation (1.1) acquires particular geometric significance is acquired when $1 - c = 1/p$, $c - a - b = 1/q$ and $a - b = 1/r$ are reciprocals of integers $p, q, r \in \mathbb{Z}_{\geq 2}$. Then there exist two solutions u_1, u_2 of (1.1) such that the quotient u_1/u_2 maps the upper half plane $\mathcal{H}$ to a hyperbolic triangle, also in $\mathcal{H}$, and such that analytic continuation of this quotient yields a tiling of $\mathcal{H}$. The projective monodromy group $\Delta(p, q, r)$ is then a discrete subgroup of $\mathrm{PSL}_2(\mathbb{R})$ with presentation

$$\Delta(p, q, r) = \langle \alpha, \beta, \gamma | \alpha^p = \beta^q = \gamma^r = \alpha\beta\gamma = 1 \rangle. \tag{1.2}$$

These groups are called *triangle groups*.

Fix a complex elliptic curve E. Then the Fuchsian equations on E with a single singular point (which we may assume to be at the origin) are given by

$$(y\frac{d}{dx})^2 u = (n(n+1)x + A)u, \tag{1.3}$$

where n and A are parameters.

We again consider cases when (1.3) is geometrically significant. For this, fix an integer $e \in \mathbb{Z}_{\geq 2}$, and consider the maximal covering $\pi : U \to E$ ramifying only above $0 \in E(\mathbb{C})$, of index e. (This covering exists in the category of Riemann surfaces, though not in the category of algebraic curves.) Then the general theory of uniformizing differential equations shows:

(i) $U \cong \mathcal{H}$.
(ii) The map π can be identified with the projection $\mathcal{H} \to \Gamma\backslash\mathcal{H}$ for some discrete $\Gamma \in \mathrm{PSL}_2(\mathbb{R})$.

Date: August 27, 2011.

(iii) For $n = \frac{1}{2e} - \frac{1}{2}$ and for *some* A, there is a quotient of two solutions u_1, u_2 of (1.3) mapping E to a quadrilateral in $\mathcal{H}$. The multivalued inverse map π^{-1} is given by the analytic continuation of this quotient.

(iv) For the above choice of A, the projective monodromy group of Γ can be identified with Γ. The group Γ has presentation

$$\Gamma = \langle \alpha, \beta, \gamma | \gamma = [\alpha, \beta], \gamma^e = 1 \rangle. \tag{1.4}$$

Finally, one can prove, using Rankin-Cohen brackets, that one of the solutions of (1.3) is then given by a meromorphic modular form for Γ.

We call the group Γ occurring above $(1; e)$-groups. The correspondence between Γ and the pair $(E = \Gamma\backslash\mathcal{H}, A)$ is a special instance of the classical *accessory parameter problem*, for which no general methods exist as of yet. We restrict our attention further by taking a small detour.

2. Arithmeticity

Let F be a totally real number field. Let B be a quaternion algebra over F, that is, a vector space

$$B = F \oplus Fi \oplus Fj \oplus Fk \tag{2.1}$$

with F-algebra structure determined by $i^2 \in F^\times$, $j^2 \in \mathbb{F}^\times$, $ij = k = -ij$. The most well-known case is of course the Hamilton algebra $\mathbb{H}$ over $\mathbb{R}$ determined by $i^2 = -1 = j^2$.

Let $\mathcal{O}$ be an order of B, that is, a projective $\mathbb{Z}_F$-submodule of B of rank 4 that is also a ring. Suppose that

$$B \otimes_{\mathbb{Q}} \mathbb{R} \cong M_2(\mathbb{R}) \otimes \mathbb{H} \otimes \cdots \otimes \mathbb{H}; \tag{2.2}$$

this just means that except for a single embedding of F into $\mathbb{R}$, the squares i^2 and j^2 are both negative. B then embeds in the first factor of (2.2) via some ι. We identify both B and $\mathcal{O}$ with their image in $M_2(\mathbb{R})$. Set $\mathcal{O}^+ = \mathcal{O}^\times \cap \mathrm{GL}_2(\mathbb{R})^+$ (positive determinant), and let $\mathrm{P}\mathcal{O}^+$ be its image in $\mathrm{PSL}_2(\mathbb{R})$.

Definition 2.1. A subgroup of $\mathrm{PSL}_2(\mathbb{R})$ is called *arithmetic* if there exist $F, B, \mathcal{O}, \iota$ as above such that the intersection of Γ and PO^+ as finite index in both. Γ and $\mathrm{P}\mathcal{O}^+$ are then called *commensurable*. Notation: $\Gamma \sim \mathrm{P}\mathcal{O}^+$.

An example is in order. If we take $F = \mathbb{Q}$, $B = M_2(\mathbb{Q})$, $\mathcal{O} = M_2(\mathbb{Z})$ and ι the canonical embedding, then $\mathrm{P}\mathcal{O}^+ = \mathrm{P}\mathcal{O}^1 = \mathrm{PSL}_2(\mathbb{Z})$. This is the classical modular group, whose fundamental domains contain cusps.

For all non-matrix B, the fundamental domains for $\mathrm{P}\mathcal{O}^+$ do not contain cusps. This makes them prettier, but also excludes the use of Fourier expansions, making its harder to calculate with modular form on $\Gamma\backslash\mathcal{H}$.

Before resuming the main thread of our argument, let it be mentioned that in the case $F = \mathbb{Q}$, work by Shimura shows that the curve $\mathrm{P}\mathcal{O}^+\backslash\mathcal{H}$ parametrizes certain *fake elliptic curves*. That is, if we let $\mathrm{FE}(\mathcal{O})$ be the set of isomorphism classes of pairs (A, i), where A is a principally polarized abelian surface and i is a (maximal, Rosati-compatible) embedding of $\mathcal{O}$ into $\mathrm{End}(A)$, then there is a bijection

$$\begin{aligned} \mathrm{P}\mathcal{O}^+\backslash\mathcal{H} &\longrightarrow \mathrm{FE}(\mathcal{O}) \\ z &\longmapsto \mathbb{C}^2/\mathcal{O}\begin{pmatrix} z \\ 1 \end{pmatrix}. \end{aligned} \tag{2.3}$$

This connection with periods is why we call the differential equations associated with arithmetic groups *arithmetic Picard-Fuchs equations*.

3. Our objectives

Kisao Takeuchi proved in 1983 that there are 73 $(1;e)$-groups up to conjugacy. We wish to determine the pair (E,A) for these Γ. The original motivation (due to Beukers) is the extension of Apery-like irrationality results; however, the above shows that our problem is also deeply related with the determination of the Shimura curves (featured below) and with the construction of modular forms for general subgroups Γ of $\mathrm{PSL}_2(\mathbb{R})$.

We illustrate our main approaches below. Let us mention that we were able to determine the isogeny class of E in all cases, its isomorphism class in about two-thirds, and A in about one-third of them.

4. Case 1: $\Gamma \sim \Delta$

Suppose first that Γ is commensurable with a triangle group. For simplicity, we even suppose that there is an inclusion $\Gamma \subset \Delta(p,q,r)$ (this is not typical, though). After Elkies, who explored these questions in a genus 0 setting, we use the bijections between the sets consisting of the following elements:

(i) Conjugacy classes of subgroups Γ of $\Delta(p,q,r)$.
(ii) Isomorphism classes of finite morphisms $X \to \mathbb{P}^1_{\mathbb{C}}$ ramifying only above $0,1,\infty$ of index dividing p,q,r, respectively.
(iii) Conjugacy classes of finite permutation triples $(\sigma_0,\sigma_1,\sigma_\infty)$ satisfying $\sigma_0^p = \sigma_1^q = \sigma_\infty^r = \sigma_0\sigma_1\sigma_\infty = 1$.

The triple of permutations associated to an inclusion $\Gamma \subset \Delta(p,q,r)$ corresponds to the morphism

$$\Delta(p,q,r) \to \mathrm{Sym}(\Delta(p,q,r)/\Gamma) \tag{4.1}$$

induced by left multiplication.

Knowing Γ and $\Delta(p,q,r)$ explicitly enough (and Takeuchi allows us to get good grip on these groups), one can therefore employ group theory to study and simplify the calculation of the cover $X \to \mathbb{P}^1_{\mathbb{C}}$. We illustrate this in the next example. After determining the cover, one can find A in (1.3) by pulling back the equation (1.3) and then taking a suitable projective normalization.

The promised example is the following. Consider the triangle group $\Delta = \Delta(2,5,6)$. Then using permutations, one shows that there exists a unique cover of $\mathbb{P}^1_{\mathbb{C}}$ as above of degree 6 and with ramification indices $(2,2,2)$, $(5,1)$ and (6) at the points above $0,1,\infty$. Indeed, there exist permutations in the corresponding conjugacy classes of S_6 with trivial product.

Consider this cover $f : X \to PP^1$. Riemann-Hurwitz shows that X has genus 1. The quotient map from $\mathcal{H}$ to $\mathbb{P}^1_{\mathbb{C}} = \Delta\backslash\mathcal{H}$ ramifies doubly above 0. But so does f. Hence the factorization $\mathcal{H} \to X$ does not ramify at the points above 0. Arguing similarly in the other fibers, we see that $\mathcal{H} \to X$ ramifies only above the point at which f ramifies singly, which is in accordance with our geometric construction of $(1;5)$-groups.

Putting the sextuply (instead of the singly) ramifying point at infinity, f is given by

$$\frac{2^2}{5^5}(9xy - x^3 - 15x^2 - 36x + 32) \tag{4.2}$$

from the curve

$$y^2 + xy + y = x^3 + x^2 + 35x - 28. \tag{4.3}$$

5. CASE 2: $\Gamma \not\sim \Delta$

The preceding case was extremely agreeable in that we could determine the parameter A in (1.3). The method we now describe only manages to describe $E = \Gamma\backslash\mathcal{H}$. This is done by exploiting the arithmetic properties of $\Gamma\backslash\mathcal{H}$. We now suppose that Γ is a $(1;e)$-group such that $\Gamma = \mathrm{P}\mathcal{O}^+$. (Actually, this never happens, but we can pretend so for expository purposes.)

We need some notation. Let $\mathbb{A}^f$ be the finite adèle ring over $\mathbb{Q}$, let $\widehat{\mathbb{Z}}$ be the integral closure of $\mathbb{Z}$ in $\mathbb{A}^f$, and let $X = \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{R})$. Let $K = (\mathcal{O} \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}})^\times$ and consider the double quotient

$$B\times\backslash X \times (B \otimes_{\mathbb{Q}} \mathbb{A}^f)^\times / K \tag{5.1}$$

Here K acts only on the right factor of $X \times (B \otimes_{\mathbb{Q}} \mathbb{A}^f)^\times$, via left multiplication. $B^\times$ acts on $(B \otimes_{\mathbb{Q}} \mathbb{A}^f)^\times$ on the left via the diagonal embedding, and on X via the fractional linear transformations obtained via the previously chosen embedding ι.

It is then a triviality (!) to show that $\Gamma\backslash\mathcal{H}$ is isomorphic to the connected component of $\mathrm{Sh}(K)$ containing $(i, 1)$. This rephrasing may seem overly cumbersome, but it is important to describe the arithmetic properties mentioned in the next paragraph. Furthermore, when $\Gamma \neq \mathrm{P}\mathcal{O}^+$, it is sometimes necessary to use more general groups K.

We describe some arithmetic properties of $\mathrm{Sh}^0(K)$.

- **Field of definition.** There is a norm map on B and its completions that is the analogue of the determinant map on $M_2(F)$. Applying this to (5.1), one obtains a double quotient $F^\times\backslash\{\pm 1\} \times (\mathbb{A}^f)^\times/\mathrm{Nm}(K)$. Global class field theory associated a finite abelian extension H of F to this double quotient. Work by Shimura shows that the curve $\mathrm{Sh}^0(K)$ admits a model over H that is "canonical" (meaning that the points on this model generate appropriate class fields). We identify $\mathrm{Sh}^0(K)$ with this model in what follows. Let us remark that if $\mathcal{O}$ is maximal and the narrow class number of F equals 1 (such as in the case $F = \mathbb{Q}$), then $H = F$.
- **Bad primes.** By work of Carayol, these are exactly the primes of H over the primes $\mathfrak{p}$ of F where either $B \otimes_F F_{\mathfrak{p}}$ is not isomorphic to $M_2(F_{\mathfrak{p}})$ or K is not maximal.
- **Traces of Frobenius.** As in the classical modular case, the traces of Frobenius of $\mathrm{Sh}^0(K)$ can be calculated at a good prime $\mathfrak{p}$ by a purely geometrical construction. Indeed, the Eichler-Shimura relation describes a geometric correspondence that reduces mod $\mathfrak{p}$ to the Frobenius correspondence. The former correspondences can be determined once a fundamental domain for $\mathrm{P}\mathcal{O}^+$ is determined. But this is the quadrilateral mentioned earlier.
- **Valuations of j.** The valuations of $j(\mathrm{Sh}^0(K))$ at the primes of H over the primes $\mathfrak{p}$ of F such that $B \otimes_F F_{\mathfrak{p}} \not\cong M_2(F_{\mathfrak{p}})$ can be calculated using $\mathfrak{p}$-adic uniformization results by Boutot and Zink. I will not go into detail on this.

All the above data can be determined explicitly by combining the work of Takeuchi with algorithms developed by Voight. Our trick, a generalization of an idea due to Dembélé and Donnelly, is to combine them to determine $\mathrm{Sh}^0(K)$ as a genus 1 curve over H. In all our cases, we have that after calculating the number of points of $\mathrm{Sh}^0(K)$ modulo over many good primes, these numbers are all divisible by a small prime p (usually 2). So $\mathrm{Sh}^0(K)$ most likely gives rise to an H-rational point on the classical modular curve $Y_0(p)$. There are two cases.

- If $g(Y_0(p)) > 0$, then these H-points are either a finite set or a finitely generated group. Browsing through them quickly gives a candidate equation for $\mathrm{Sh}^0(K)$.
- If $g(Y_0(p)) = 0$, then $Y_0(p)$ allows an equation $uj = f(u)$. Here f is a monic integral polynomial of degree $p + 1$ whose constant term is a non-trivial power of p. We can parametrize $\mathbb{G}_m \to Y_0(p)$ via $u \mapsto (u, f(u)/u)$. However, we need to do better, because $\mathbb{G}_m(H)$ is not finitely generated. For this, we simply note that u cannot have non-trivial valuation at the good primes $\mathfrak{P}$ of $\mathrm{Sh}^0(K)$ not lying above p, because we would then have $v_{\mathfrak{P}}(j) < 0$, in contradiction with the good reduction of $\mathrm{Sh}^0(K)$. This cuts down the parametrization of H-points to a finitely generated group, allowing us once more to quickly find a candidate equation.

Of course, we have to prove that the resulting candidate for $\mathrm{Sh}^0(K)$ is correct. A result by Faltings and Serre can be used to verify the correctness of the isogeny class by computing only finitely many traces of Frobenius. The isomorphism classes in this isogeny class can then be calculated effectively by using a result of Dieulefait and Dmitrov. If only one isomorphism class has the correct valuations of j, then we have found a correct equation.

This method is rather indirect. . .

6. Final comments

Some interesting question remain, for example:

(i) When does the model $\mathrm{Sh}^0(K)$ for $\Gamma\backslash\mathcal{H}$ determine on the choice of K?

(ii) How can one efficiently determine the parameter A in Case 2 above? Previous work was done by Elkies, and Hoefmann, Van Straten and Yang have developed numerical methods.

Finally, the reader who is interested can experiment with our methods himself, using the `Magma` programs at `http://sites.google.com/site/sijsling/programs`.