Computing Puiseux Expansions at Cusps of the Modular Curve $X_0(N)$

Mark van Hoeij*
Florida State University, Tallahassee, FL 32306-3027, USA
hoeij@math.fsu.edu

July 8, 2013

1 Notation

The function field of the modular curve $X_0(N)$ can be written as $\mathbb{C}(x_1)[x_2]/(\phi_N)$ where $\phi_N \in \mathbb{Z}[x_1, x_2]$ satisfies $\phi_N(j(\tau), j(N\tau)) = 0$. A place P corresponds to a discrete valuation v_P on the function field ($v_P(g) < 0$ means that a function g has a pole at P, and $v_P(g) > 0$ means a root, of that order). The cusps are the places P where x_1, x_2 have poles.

Goal: An efficient algorithm to compute Puiseux expansions at cusps of $X_0(N)$.

A Puiseux expansion at a cusp P of $X_0(N)$ can be written as

$$x_1 = t^{-d}, \qquad x_2 = c_0 \cdot t^{-n} \cdot (1 + \cdots) \ \in \ \mathbb{Z}[c_0, d^{-1}][[\, t\,]]. \tag{1}$$

Here n, d are positive integers, c_0 is a root of unity, t is a local parameter at P, and the dots refer to terms with positive powers of t. To avoid negative exponents, we switch to the variables

$$x = \frac{1}{x_1} = \frac{1}{j(\tau)}, \quad \text{and} \quad h = \frac{1}{x_2} = \frac{1}{j(N\tau)}.$$

Now x, h satisfy an algebraic relation $P_N(x, h) = 0$ that is trivially obtained from ϕ_N by substituting $(x_1, x_2) \mapsto (x^{-1}, h^{-1})$. However, ϕ_N and P_N are not needed for computing a Puiseux expansion at a cusp.

In terms of x, h the Puiseux expansion (1) looks like

$$x = t^d, \quad h = c \cdot t^n \cdot (1 + \cdots)$$

*Supported by NSF grant 1017880.

where $c = 1/c_0$. We can rewrite that to (from now on we will use this form):

$$h = c \cdot x^q \cdot (1 + \cdots) \ \in \ \mathbb{Z}[c, d^{-1}][[\, x^{1/d} \,]] \tag{2}$$

where $q = \frac{n}{d}$ is a positive rational number. We will call

$$T := c \cdot x^q$$

the *initial term* of h. We are only interested in those h for which $\exists_N P_N(x, h) = 0$. Such h turn out (see Section 3) to be uniquely determined by their initial term. Section 1.2 will explain how to find N from T.

1.1 Puiseux series

Let

$$\hat{K} := \bigcup_{d=1}^{\infty} \mathbb{C}((x^{1/d}))$$

denote the field of Puiseux series over $\mathbb{C}$. If $\alpha \in \hat{K} - \{0\}$, then $v(\alpha) \in \mathbb{Q}$ denotes the exponent of the initial term. So

$$v(h) = v(T) = q.$$

Definition 1. *Let $a \in \frac{1}{d}\mathbb{Z}$ and h as in (2). By computing h to* precision *a we mean computing the factor $(1 + \cdots)$ mod x^a, and hence h mod x^{q+a}.*

Input and output of our algorithm. Given h up to precision a, we will show that h can be computed quickly to precision $2a$. Starting with the initial value $cx^q(1 + O(x^{1/d}))$, we will thus find h mod $x^{q+d^{-1}2^k}$ after k steps.

1.2 The number N

For any monomial $T = cx^q$, with c a root of unity, and q a positive rational number, our algorithm will compute a specified number of terms of a Puiseux series $h = T \cdot (1 + \cdots)$ for which $P_N(x, h) = 0$ for one N. We can quickly determine N from T. For instance, if N is prime, then either $(c, q) = (1, N)$ or $(c, q) = (\zeta_N^s, 1/N)$ for some $s \in \{0, \ldots, N-1\}$. The relation between other N's and their T's comes from composition, as shown in these examples:

Example 1. *Composing $T = \pm x^{1/2}$ and $T = x^2$ (all belonging to $N = 2$) we obtain x and $-x$. Now $T = x$ belongs to $N = 1 = 2/2$, but $T = -x$ does not. So it must belong to $N = 2 \cdot 2 = 4$. Similarly, ix^2 (where $i = \zeta_4 = \sqrt{-1}$) belongs to $X_0(2^k)$ for some k since it can be obtained by repeated compositions of x^2 and $\pm x^{1/2}$. Here k must be 5 since we do not obtain ix^2 by composing fewer than 5 functions from $\{x^2, \pm x^{1/2}\}$. In contrast, $T = ix^{1/2}$ belongs to $N = 2^3$.*
Likewise, $-x^{1/3}$ and $x^{3/4}$ can only belong to $N = 3 \cdot 2^2 = 12$, because both require compositions involving 1 element from $\{x^3, \zeta_3^* x^{1/3}\}$ and 2 elements from $\{x^2, \pm x^{1/2}\}$. Likewise, $T = x^{5/3}$ and $T = \zeta_3 x^{5/3}$ belong to $N = 15$, and $T = \zeta_5 x$ belongs to $N = 25$.

2 A relation between x and h

The reciprocals of x and h satisfy the modular equation ϕ_N. Since ϕ_N can be large when N is large, we will use another relation between x and h, one that is valid for any N. Define $E, F, G \in \mathbb{Z}[[x]]$ as

$$E := x \cdot \sqrt{1 - 1728\,x}, \quad F := {}_2\mathrm{F}_1\left(\left.\begin{matrix}\frac{1}{12}, \frac{5}{12} \\ 1\end{matrix}\right| 1728\,x\right)$$

and

$$G := E \cdot F^2 = E \cdot {}_3\mathrm{F}_2\left(\left.\begin{matrix}\frac{1}{6}, \frac{1}{2}, \frac{5}{6} \\ 1, 1\end{matrix}\right| 1728\,x\right).$$

G satisfies a linear homogeneous differential equation L_3 over $\mathbb{Q}(x)$

$$L_3: \quad G''' + a_2 G'' + a_1 G' + a_0 G = 0$$

with $a_0, a_1, a_2 \in \mathbb{Q}(x)$. The factor E in G was selected to ensure $a_2 = 0$.

The following relation

$$v(h) \cdot G \circ h = h' \cdot G \tag{3}$$

holds for every $h \in \hat{K}$ for which $\exists_N P_N(x, h) = 0$. We computed this relation by reformulating the condition [To Do: Find reference] that $F \circ h$ should be an algebraic function times F. The projective monodromy matrices of F are precisely the famous generators of the modular group PSL(2,$\mathbb{Z}$).

Section 3 shows that for any positive rational number q and any $c \in \mathbb{C} - \{0\}$ there exists precisely one $h \in \hat{K}$ that satisfies (3) and has cx^q as its initial term. This h is algebraic over $\mathbb{C}(x)$ iff[1] c is a root of unity.

3 Computing h from its initial term

Differentiating (3) and dividing by h' we find

$$v(h) \cdot G' \circ h = G \cdot \left(\frac{h''}{h'} + \frac{G'}{G}\right) = G \cdot \mathrm{ld}(h'G) \tag{4}$$

where ld denotes the logarithmic derivative, $\mathrm{ld}(u) := \ln(u)' = u'/u$. Suppose that h_0 is an approximation of h with $v(\epsilon) \geqslant a + v(h) > a$ where ϵ denotes $h - h_0$. Substituting $h = h_0 + \epsilon$ in (3) and (4) gives

$$(h_0' + \epsilon') \cdot G = v(h) \cdot G \circ (h_0 + \epsilon) = v(h) \cdot (G \circ h_0 + \epsilon \cdot (G' \circ h_0) + O(\epsilon^2)) \tag{5}$$

and, using $v(G) = 1$,

$$v(h) \cdot G' \circ h_0 + O(\epsilon) \;=\; G \cdot \mathrm{ld}(h_0' G) + O(x^a). \tag{6}$$

[1]The fact that h satisfies some P_N when c is a root of unity implies that h can not be algebraic when c is not a root of unity. If c is not a root of unity, and if h were algebraic, then $c \equiv \zeta_N \bmod p$ for a large N and a large prime p, and we would get arbitrarily high lower bounds on the algebraic degree of h reduced mod p, leading to a contradiction.

Substituting (6) into (5), dividing by G, then subtracting h_0', gives

$$\epsilon' = \frac{v(h) \cdot (G \circ h_0)}{G} + \epsilon \cdot \mathrm{ld}(h_0' G) - h_0' \ + O(x^{v(h)+2a-1}).$$

Now $\epsilon' = \mathrm{ld}(A)\epsilon + B + O(x^s)$ has a solution $\epsilon = A \int B/A \ + O(x^{s+1})$, applying that gives

$$\epsilon = h_0' G \int \frac{1}{G} \left(\frac{v(h) \cdot (G \circ h_0)}{h_0' G} - 1 \right) \mathrm{d}x \ + O(x^{v(h)+2a}). \tag{7}$$

Adding this to h_0 doubles the precision in the sense of Definition 1.

Algorithm PuiseuxX0N.

Input: $T = cx^q$ where c is a root of unity and q a positive rational number, and a positive integer k.

Output: An approximation of precision $d^{-1}2^k$ (as in Definition 1) of a Puiseux series h with initial term T that satisfies $P_N(x, h) = 0$ (with N as in Example 1).

Step 1. $h_0 := T$ and $a := d^{-1}$ where $d = \text{denominator}(q)$.
Step 2. Repeat k times:
 (a) Compute ϵ mod x^{q+2a} with formula (7).
 (b) $h_0 := h_0 + \epsilon$ and $a := 2a$.
Step 3. Return h_0.

A Maple implementation is given at `www.math.fsu.edu/~hoeij/files/X0N`, in the file `PuiseuxX0N`. The CPU time is dominated by the cost of composing $G \circ h_0$. Now G contains F^2, so we must compose a ${}_2F_1$ function with a truncated power series h_0. Brent and Kung [1] described an algorithm that can perform this step efficiently. This, combined with fast arithmetic in $\mathbb{Z}[c, d^{-1}]$, reduces the computational complexity to quasi-linear time (logarithmic factors times the size of the output).

One could compute ϕ_N by (i) computing Puiseux expansions to sufficient precision, and then (ii) reconstructing ϕ_N from them. Step (i) is quasi-linear, and so is Step (ii) if N is for example a power of 2. But if N contains large prime(s), it is not clear if Step (ii) can be done faster than [2].

References

[1] R. P. Brent, H. T. Kung, *Fast Algorithms for Manipulating Formal Power Series*, J. ACM, **25**, No. 4, p. 581-595 (1978).

[2] R. Bröker, K. Lauter, A. Sutherland, *Modular polynomials via isogeny volcanoes*, Math. Comp. **81**, p. 1201-1231 (2012).