Points in $\mathfrak{h}$ corresponding to level N structures

Math 581g project, Joe Pacold

December 13, 2011

1 Introduction

As part of the discussion of modular curves in this course, we studied the following correspondence between elliptic curves with attached level N structures and points in the complex upper half plane $\mathfrak{h}$. For $\tau \in \mathfrak{h}$, let Λ_τ be the lattice $\mathbb{Z} + \mathbb{Z}\tau$, and let E_τ be the elliptic curve $\mathbb{C}/\Lambda_\tau$. For any elliptic curve E over $\mathbb{C}$,

(a) If C is a cyclic subgroup of E of order N, there exists $\tau \in \mathfrak{h}$ such that $E \approx E_\tau$ and the isomorphism maps C to the subgroup of E_τ generated by $1/N$.

(b) If $P \in E$ has order N, then there exists $\tau \in \mathfrak{h}$ such that $E \approx E_\tau$ and the isomorphism maps P to $1/N$.

(c) If $P, Q \in E$ and $e(P,Q) = -1$ (where e is the Weil pairing), then there exists $\tau \in \mathfrak{h}$ such that $E \approx E_\tau$ and the isomorphism maps P to $1/N$ and Q to τ/N.

Following the proof of these statements given in the course (Proposition 5.2.8 in [1]), we can explicitly compute τ for a given E and a given level N structure by this procedure:

1. Compute $\omega_1, \omega_2 \in \mathbb{C}$ such that $E \approx \mathbb{C}/(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2)$, i.e. so that $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ is the period lattice of the invariant differential ω attached to E.
2. Determine the point(s) in $\mathbb{C}/(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2)$ corresponding to the level N structure.
3. Make a change of basis from $\langle \omega_1, \omega_2 \rangle$ to $\langle \omega_1', \omega_2' \rangle$ so that (a) C maps to the cyclic group generated by ω_1'/N, (b) P maps to ω_1'/N, or (c) P maps to ω_1'/N and Q maps to ω_2'/N.
4. Change basis from $\langle \omega_1', \omega_2' \rangle$ to $\langle 1, \tau = \pm\omega_2'/\omega_1' \rangle$, choosing the sign so that $\mathrm{Im}(\tau) > 0$.

The proof from class implies an algorithm for steps 3 and 4, so here I will focus on steps 1 and 2. Section 2, based on Ch. VI of [2], describes a procedure for the first two steps that uses line integrals of the differential ω over suitably chosen paths. Section 3 discusses the method already implemented in Sage, which uses connections between arithmetic-geometric sequences, chains of lattices in $\mathbb{C}$, and chains of 2-isogenies of elliptic curves.

2 Line integral method

Given an elliptic curve E over $\mathbb{C}$, we begin by changing variables so that its Weierstrass equation has the form

$$E : y^2 = x(x-1)(x-\lambda) \tag{1}$$

where $\lambda \neq 0, 1$ (since E must be smooth). The complex points on E then lie on a torus, which can be viewed as two copies of $\mathbb{C}$ joined along some choice of branch cuts for the differential $\omega = dx/y = dx/\sqrt{x(x-1)(x-\lambda)}$ attached to E. The conventional branch cut for the square root function (along the negative real axis) leads to a natural choice of branch cuts for ω: if λ is real and $\lambda < 0$, we take one branch cut along the negative real axis from $-\infty$ to λ, and another along the real axis from 0 to 1. Otherwise, we let one cut join $-\infty$ and 0 and let the other join 1 and λ.

By numerically integrating ω over two paths that circle the torus in different directions (Fig. 1), we can compute $\omega_1, \omega_2 \in \mathbb{C}$ such that the torus is isomorphic to $\mathbb{C}/(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2)$. In addition, given $P = (x_P, y_P) \in E$, we can compute the point in $\mathbb{C}/(\mathbb{Z}\omega_1+\mathbb{Z}\omega_2)$ corresponding to P by integrating ω along any path from the point at infinity to x_P. To ensure that the integral converges, it is convenient to use the path

$$x(t) = \mathrm{Re}(x_P) + it, \quad \infty > t \geq \mathrm{Im}(x_P),$$

so that

$$\begin{aligned} P \longmapsto \int_O^P \omega &= \int_O^P \frac{dx}{\sqrt{x(x-1)(x-\lambda)}} \\ &= \int_\infty^{\mathrm{Im}(x_P)} \frac{i\,dt}{\sqrt{(\mathrm{Re}(x_P)+it)(\mathrm{Re}(x_P)+it-1)(\mathrm{Re}(x_P)+it-\lambda)}} \end{aligned} \tag{2}$$

As $t \to \infty$, the integrand is of order $t^{3/2}$, so the integral converges.

Before numerically performing any of these integrals it is necessary to check whether the path crosses either of the branch cuts (or equivalently, whether the quantity under the square root crosses the negative real axis). If so, the path must be broken up so that each piece lies on only one branch of the integrand. This is straightforward when λ is real, but somewhat difficult to do for a general $\lambda \in \mathbb{C}$.

As an example, let E have the Weierstrass equation $y^2 = x(x-1)(x+3)$. The natural branch cuts join -3 to $-\infty$ and 0 to 1, so to compute a basis for the period lattice we first integrate around one branch cut:

$$\begin{aligned} \omega_1 = \lim_{\epsilon\to 0}\left(\int_{-\infty}^{-3} \frac{dt}{\sqrt{(t+i\epsilon)(t+i\epsilon-1)(t+i\epsilon+3)}} + \lim_{\epsilon\to 0}\int_{-3}^{-\infty} \frac{dt}{\sqrt{(t-i\epsilon)(t-i\epsilon-1)(t-i\epsilon+3)}}\right) \\ \approx -3.3715i \end{aligned}$$

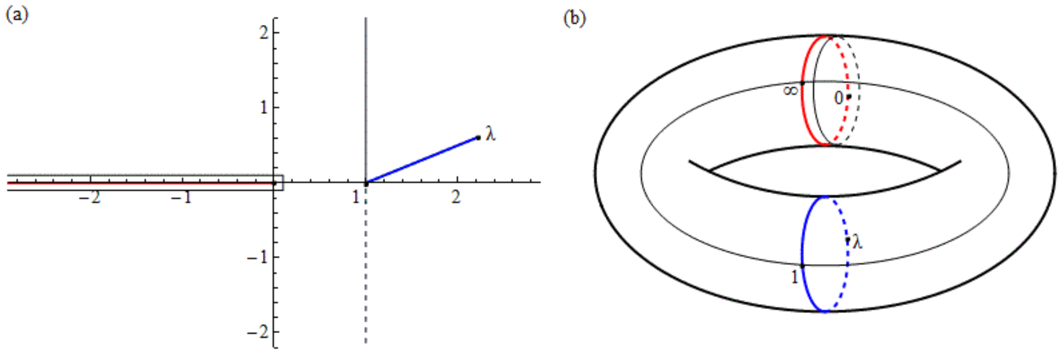

Figure 1: (a) Branch cuts in the complex plane for the differential dx/y attached to the elliptic curve $E : y^2 = x(x-1)(x-\lambda)$, with integration paths to compute a basis for the period lattice. (b) Two copies of $\mathbb{C}$ joined to form a torus, with the integration paths from (a) shown. Note that the path joining 1 and the point at infinity includes a piece on each branch of dx/y.

We then integrate from 0 to the point at infinity and back, using a different branch for each part of the integral:

$$\omega_2 = \int_{-\infty}^{0} \frac{i\ dt}{-\sqrt{it(it-1)(it+3)}} + \int_{0}^{\infty} \frac{i\ dt}{\sqrt{it(it-1)(it+3)}} \approx -4.31303$$

The point $P = (3,6) \in E$ has order 4. The corresponding complex number is given by integrating dx/y from $3 + i\infty$ to 3, breaking up the integral at the point $x = 3 + 6i$ (where y crosses the negative real axis):

$$P \mapsto \int_{\infty}^{6} \frac{idt}{-\sqrt{(3+it)(3+it-1)(3+it+3)}} + \int_{6}^{\infty} \frac{idt}{+\sqrt{(3+it)(3+it-1)(3+it+3)}} \approx -1.07826$$

This is $(1/4)\omega_2$, so we change basis from $\langle \omega_1, \omega_2 \rangle$ to $\langle 1, -\omega_1/\omega_2 \rangle$ and conclude that

$$(E, P) \approx (E_\tau, P_\tau) \text{ with } \tau \approx 1.27926i.$$

3 Arithmetic-geometric mean sequence method

If E is an elliptic curve, the existing Sage command

```
sage: E.period_lattice(CC)
```

returns the lattice in $\mathbb{C}$ corresponding to E, and

```
sage: E.period_lattice(CC).basis()
```

returns a numerical approximation to a basis for the lattice. In addition, for $P \in E$,

```
E.period_lattice(CC).elliptic_logarithm(P)
```

returns the point in $\mathbb{C}/(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2)$ corresponding to P. Each calculation is performed by taking the limit of an appropriately chosen sequence, as described in [3] and sketched here.

A *lattice chain (of index 2)* is a sequence of lattices $\Lambda_n \subset \mathbb{C}$ such that

1. $\Lambda_n \supset \Lambda_{n+1}$ for all $n \geq 0$,
2. $[\Lambda_n : \Lambda_{n+1}] = 2$ for all $n \geq 0$, and
3. $\Lambda_n + 1 \neq 2\Lambda_{n-1}$ for all $n \geq 1$.

A *good lattice chain* is a lattice chain in which $\Lambda_{n+1} = \langle\omega\rangle + 2\Lambda_n$, with ω an element of $\Lambda_n - 2\Lambda_{n-1}$ with minimal absolute value, for all but finitely many n. It is possible to show that a lattice chain is good if and only if the intersection

$$\Lambda_\infty = \bigcap_{n=0}^{\infty} \Lambda_n$$

has rank 1. Furthermore, if ω_∞ is a generator of Λ_∞ for a good chain, then it is a primitive element of Λ_0, i.e. there is some $\omega_2 \in \Lambda_0$ such that $\langle\omega_\infty, \omega_2\rangle = \Lambda_0$. It then follows that $\Lambda_n = \langle\omega_\infty, 2^n\omega_2\rangle$ for all $n \geq 0$. Now, the Weierstrass $\wp$-function associated to Λ_n is

$$\begin{aligned} \wp_{\Lambda_n}(z) &= \frac{1}{z^2} + \sum_{0\neq\omega\in\Lambda_n} \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \\ &= \frac{1}{z^2} + \sum_{\substack{r,s\in\mathbb{Z} \\ (r,s)\neq(0,0)}} \frac{1}{(z-(r\omega_\infty + s2^n\omega_2))^2} - \frac{1}{(r\omega_\infty + s2^n\omega_2)^2} \end{aligned}$$

As $n \to \infty$, all the terms with $s \neq 0$ vanish, leaving

$$\begin{aligned} \lim_{n\to\infty} \wp_n(z) &= \sum_{r\in\mathbb{Z}} \frac{1}{(z - r\omega_\infty)^2} - \sum_{0\neq r\in\mathbb{Z}} \frac{1}{(r\omega_\infty)^2} \\ \wp_\infty(z) &= \left(\frac{\pi}{\omega_\infty}\right)^2 \frac{1}{\sin^2(z\pi/\omega_\infty)} - \frac{\pi^2}{3\omega_\infty^2} \qquad (3) \end{aligned}$$

This suggests that, given a sequence of elliptic curves E_n with period lattices Λ_n that form a good chain, we could compute at least one element of a basis for Λ_0 by looking at the limit of the Weierstrass equations for the E_n.

It turns out that we can construct the required elliptic curves from an appropriately chosen arithmetic-geometric mean sequence. An *AGM sequence* is a sequence of ordered pairs $(a_n, b_n) \in \mathbb{C}^2$ $(n \geq 0)$ such that $a_n, b_n \neq 0$, $a_n^2 \neq b_n^2$, and

$$a_{n+1} = \frac{a_n + b_n}{2}, \quad b_{n+1} = \pm\sqrt{a_n b_n}$$

for all n. The sequence is said to be *good* if the signs of the b_n are chosen so that $\mathrm{Re}(b_n/a_n) \geq 0$ for all but finitely many n. It is possible to show that a good AGM sequence converges, and that $\lim_{n\to\infty} a_n = \lim_{n\to\infty} b_n \neq 0$. We will denote this limit by $M_S(a_0, b_0)$, where $S = \{n \in \mathbb{Z}_{\geq 0} : \mathrm{Re}(b_n/a_n) < 0\}$ is the set of "bad" indices.

Given a good AGM sequence (a_n, b_n), consider the sequence of elliptic curves E_n defined over $\mathbb{C}$ by

$$E_n : y^2 = 4x(x + a_n^2)(x + b_n^2)$$

By direct calculation we can check that the point $P_n = (a_n b_n, 2a_n b_n(a_n + b_n)) \in E_n$ has order 4, since $2P_n = (0, 0) = T_n$. Roughly speaking, we can explicitly write down a sequence of 2-isogenies $\varphi_n : E_n \to E_{n-1}$ such that $\varphi(P_n) = T_{n-1}$, and such that the corresponding lattices form a good lattice chain as defined above. However, instead of working directly with E_n, however, we make a shift in x and work with the isomorphic elliptic curve E'_n with Weierstrass equation

$$E'_n : y^2 = 4(x - e_1^{(n)})(x - e_2^{(n)})(x - e_3^{(n)})$$

$$e_1^{(n)} = \frac{a_n^2 + b_n^2}{3}, \quad e_2^{(n)} = \frac{a_n^2 - 2b_n^2}{3}, \quad e_3^{(n)} = \frac{b_n^2 - 2a_n^2}{3}$$

This shift was chosen to set $e_1^{(n)} + e_2^{(n)} + e_3^{(n)} = 0$, so that

$$\wp_{\Lambda_n}(\omega_1^{(n)}/2) = e_1^{(n)}, \tag{4}$$

where $\omega_1^{(n)}$ is one of the periods of $\wp_{\Lambda_n}$. For $n \geq 1$, we can then define a 2-isogeny $\varphi'_n : E'_n \to E'_{n-1}$ by

$$\varphi_n(x, y) = \left(x + \frac{(e_3^{(n)} - e_1^{(n)})(e_3^{(n)} - e_2^{(n)})}{x - e_3^{(n)}}, y\left(1 - \frac{(e_3^{(n)} - e_1^{(n)})(e_3^{(n)} - e_2^{(n)})}{(x - e_3^{(n)})^2}\right)\right).$$

It is then possible to show that $\varphi_n^*(d\omega_{n-1}) = d\omega_n$, from which it follows that the φ_n commute with the isomorphisms $(\wp, \wp') : \mathbb{C}/\Lambda_n \to E'_n$ and the natural maps $\mathbb{C}/\Lambda_n \to \mathbb{C}/\Lambda_{n-1}$. Finally, from Eqs. (3) and (4) and the definition of the E'_n, we can conclude that

$$\omega_\infty = \pm\pi/M_S(a_0, b_0).$$

This means that we can compute a basis for a given E by choosing a_0 and b_0 such that $E_0 \approx E$ and taking the limit of the resulting AGM sequence. To compute another element of the basis, we permute the $e_i^{(n)}$ in the definition of φ_n.

This procedure is generally faster than the numerical integration approach, and the precision is easier to control, since AGM sequences converge rapidly. Using the same curve and point as in the previous section,

```
sage: def_lattice_tau(E,N,P):
....:     L = E.period_lattice(CC)
....:     omega = L.basis()
....:     [a,b] = L.coordinates(L.elliptic_logarithm(P))
....:     [a,b] = [ int(round(N*a)), int(round(N*b)) ]
....:
....:     while gcd(a,b)!=1 or b==0: b += N
....:     d = inverse_mod(a,b)
....:     c = (a*b - 1)/b
....:     tau = ( c*omega[0] + d*omega[1] )/( a*omega[0] + b*omega[1] )
....:     tau = tau - floor(real_part(tau))
....:
....:     return tau
....:
sage: E = EllipticCurve([0,2,0,-3,0])
sage: lattice_tau(E,4,E(3,6))
0.710057309320031 - 0.0416309862711467*I
```

4 References

1. K.A. Ribet and W.A. Stein, *Lectures on Modular Forms and Hecke Operators.*

2. J.H. Silverman, *The Arithmetic of Elliptic Curves.*

3. J.E. Cremona and T. Thongjunthug, "The complex AGM, periods of elliptic curves over C and complex elliptic logarithms" [arXiv:1011.0914v1]