Primer on elliptic curves

1. The first issue of naturality.

When we consider the natural permutation representation on a four element set S, there is for each group element g the 'twisted' representation ${}^gS$, defined by the operation $\cdot^g$ so that

$$h \cdot^g s = g^{-1}hg \cdot s.$$

The restriction of the representation to the Klein four-group maps the 24 different twisted representations to six representations of the Klein four-group.

Correspondingly, any four-sheeted cover of a complex manifold M has a natural associated six sheeted cover $\widetilde{M} \to M$ with Galois group S_4/K_4.

The holomorphic fiber bundles with fiber a Riemann sphere with four points deleted are classified by complex manifolds M together with a S_4/K_4-equivariant period map $\widetilde{M} \to \mathbb{P}^1 \setminus \{0, 1, \infty\}$. The fundamental group of $P^1 \setminus \{0, 1, \infty\}$ is the pure braid group on four strands on $\mathbb{P}^1$ and in the connected case equivariance under S_4/K_4 extends the induced map on fundamental groups to a map from the fundamental group of M to the full braid group.

For simplicity let's look at the case when M is connected. The connected components of $\widetilde{M}$ are naturally isomorphic to each other, and each connected component is a copy of the lowest cover where the period map becomes well-defined. If M is a connected curve, this is the 'Riemann surface' of the multivalued period map on M, let us call it λ, and there is a Galois field extension $\mathbb{C}(M) \subset \mathbb{C}(M, \lambda)$ whose Galois group is the stabilizer of one connected component of $\widetilde{M}$.

That is to say,

1. Remark. The period map underlying a fiber bundle with fibers Riemann spheres with four points deleted needn't be single-valued; it can be multivalued, defining a covering space of the base manifold M of degree at most six.

2. Second issue of naturality.

Another issue of naturality is this: given an elliptic curve J with chosen point p, the subgroup $2H_1(J) \subset H_1(J) \cong \pi_1(J,p)$ defines a natural four sheeted regular cover $\widetilde{J} \to J$. The inverse image of p is a four-element subset of $\widetilde{J}$ which is a torsor for unique Klein four subgroup of any of the four group structures of $\widetilde{J}$ which correspond to a choice of lift of p.

There is a unique involution of $\widetilde{J}$ with this four element subset as its fixed point set, and the quotient modulo the involution is a Riemann sphere with four marked points.

From the previous section we can associate to any fiber bundle of elliptic curves with a (chosen) section (which is possibly disconnected even if M is connected) a Galois cover $\widetilde{M} \to M$ of degree six and a S_4/K_4 equivariant period map $\widetilde{M} \to \mathbb{P}^1 \setminus \{0, 1, \infty\}$.

The corresonding four-sheeted cover of $\widetilde{M}$ can be nontrivial, it has a globally-defined free K_4 action. Pulling back along our cover of the base manifold $\widetilde{M} \to M$ allows that the twists of the K_4 torsor in each of the elliptic curve fibers are all isomorphic. Under the covering maps $\widetilde{J} \to J$ these all become identified with one basepoint in each elliptic curve fiber J.

3. The third issue of naturality.

Finally for holomorphic bundles of elliptic curves which may not have a section, and for which we have chosen no section, we must specify a complex manifold M and a bundle J of pointed elliptic curves, and an element $H^1(M, J)$ to choose a torsor. Thus

2. Theorem. A holomorpic bundles of elliptic curves (without chosen basepoint in each) is uniquely determined by choosing a complex manifold M, a four-sheeted cover of M, an S_4/K_4-equivariant period map $\widetilde{M} \to \mathbb{P}^1 \setminus \{0, 1, \infty\}$, where $\widetilde{M}$ is the corresponding six-sheeted cover, and finally an element of $H^1(M, J)$ where J is the corresponding bundle of pointed elliptic curves.

3. Corollary. In a bundle of elliptic curves which is compact and projective all elliptic curve fibers are isomorphic to each other.

Once M and therefore $\widetilde{M}$ are compact and projective, the holomorphic period map $\widetilde{M} \to \mathbb{P}^1 \setminus \{0, 1, \infty\}$ is proper and has compact image. The compact subsets of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ however are discrete.

In the next section we'll consider the universal family of elliptic curves, classified by the period map which is the identity function $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ viewed as an S_4/K_4 equivariant map. At the point where we consider the regular six-sheeted cover, we will find this can be compactified to make a smooth surface by adjoining twelve boundary Riemann spheres with normal bundle degree -2, touching in two points in pairs, one pair each lying above $\{0, 1, \infty\}$.

Once the compactification is done, the Galois action will be analytic but not algebraic. Reducing modulo the action of S_4/K_4 there results an analytic compactification of the universal bundle of elliptic curves corresponding to the j invariant by adjoining a pair of Riemann spheres of normal bundle degree -2 touching at two points, and a smooth degree six branched cover which has structure of a complex projective variety.

4. Algebraic compactification.

A corollary is a start on exercise 17 on page 25 of the Park City notes on surfaces by Miles Reid, in case $a = 1$. Note that the relation with the modular group is that $\Gamma(2)$ is the fourth pure braid group of the Riemann sphere.

Let $b \in \mathbb{P}^2$ be a point, and let $C \subset P^2$ be a curve of degree four which does not pass through b. Consider the the pencil F_1 of projective lines through b considered disjoint from each other (a ruled surface), and its map to $\mathbb{P}^1$ viewed as the set of projective lines through b. Take as M the projective line with those points deleted which correspond to lines that fail to meet C transversely. Take as $\phi : \pi_1(M, m) \to S_4$ the monodromy action on the four points of intersection of m (viewed as a line) with C. Let $\widetilde{M}$ be the covering whose Galois group is the image G of $\pi_1(M, m)$ in S_4/K_4. The G-equivariant period map $\lambda : \widetilde{M} \to \mathbb{P}^1 \setminus \{0, 1, \infty\}$ extends to a finite map from the completion of $\widetilde{M}$ to $\mathbb{P}^1$. Let L be the line bundle on F_1 whose section sheaf is the dual of the defining ideal of the curve C in F_1. There is a line bundle N such that $N^{\otimes}2 = L$ and a section s of L whose zero variety defines the union of four lines.

5. Corollary. The inverse image of the image $s(F_1)$ in N under the tensor square map is a complete projective variety which is a compactification of the bundle of elliptic curves defined by the period map λ.

4. Main example. Take as C the union of four general lines not passing through b. We can consider these lines as sections of a line bundle with section sheaf isomorphic to $\mathcal{O}(1)$.

A natural such sheaf is the sections of the one-forms on $\mathbb{P}^1$ with at most simple (=logarithmic) poles at $0, 1, \infty$ and nowhere else. Such sections are bijective with modular forms of weight 2 for $\Gamma(2)$. We let M_2 be the corresponding line bundle on $\mathbb{P}^1$.

Thus let e_1, e_2, e_3, e_4 be four modular forms for $\Gamma(2)$ of weight two. We can cover F_1 by the open sets U and V where U is the total space of

M_2 and V is the complement of the union of the section images

$$e_1(\mathbb{P}^1) \cup e_2(\mathbb{P}^1) \cup e_3(\mathbb{P}^1) \cup e_4(\mathbb{P}^1),$$

so

$$F_1 = U \cup V.$$

For each integer k, let $\mathcal{M}_k$ be the sheaf of sections of M_k. To be precise, although this only affects odd values of k which will not be relevant here, we should lift $\Gamma(2)$ to the subgroup of $SL_2(\mathbb{Z})$ generated by the two transformations T^2, ST^2S where $T(\tau) = 2+\tau$, $S(\tau) = -1/\tau$. Then $\mathcal{M}_k$ is the sheaf of weakly modular forms of weight k for the group $\langle T^2, ST^2S\rangle$. Let $h : F_1 \to \mathbb{P}^1$ be the structural map of F_1 as a bundle of Riemann spheres. Once pushed down along h the structure sheaf of U decomposes as a direct sum of sheaves over $\mathbb{P}^1$ as

$$h_*\mathcal{O}_U \cong \oplus_{k=0}^{\infty}\mathcal{M}_{-2k}$$

The way that we view a local section r of one of the $\mathcal{M}_{-2k}$ as a function $U \to \mathbb{C}$ is that if we are given a point $p \in U = M_2$ we choose a weakly modular form $f(\tau)$ of weight $2k$ passing through p and then we define $r(p)$ to mean $r(\tau)f(\tau)^k$ for τ chosen such that $\lambda(\tau) = p$. Although neither factor $r(\tau)$ nor $f(\tau)$ is a well-defined function on $\mathbb{P}^1$, the product is, and so if we consider r, f as multi-valued functions on $\mathbb{P}^1$ we can take

$$r(p) = r(h(p))f(h(p))^k.$$

This description works for all points $p \in U$ including when $h(p) \in \{0, 1, \infty\}$, and so if we use the description using τ, we are allowed to let the values of τ include ideal points.

The defining ideal sheaf of each image $e(\mathbb{P}^) \subset F_1$ restricts on V to $\mathcal{O}_V$, and on U it restricts to

$$(e_1^{-1} - 1)\mathcal{O}_{F_1}(-Z)$$

where $Z \subset M_2$ is the image of the zero section. This is because the rational function $e_1^{-1} - 1$ has a zero of order 1 the image of e_1 and a pole of order 1 on Z. Therefore the defining ideal sheaf $\mathcal{I}$ of the union of the four lines within F_1 is

$$\mathcal{I} = (e_1^{-1} - 1)(e_2^{-1} - 1)(e_3^{-1} - 1)(e_4^{-1} - 1)\mathcal{O}_{F_1}(-4Z).$$

It is not principal because the zero-section of $M_2 \subset F_1$ is not a principal divisor in F_1.

The dual coherent sheaf of $\mathcal{I}$ is the section sheaf of a line bundle L, and because the divisor class is a multiple of 2 there is a line bundle N on F_1 such that $N^{\otimes 2} = L$.

Also L has a section s whose intersection with the zero-section F_2 is the union of the e_i each with multiplicity one. The inverse image of s under the tensor square operation

$$N \to N^{\otimes 2} \cong L$$

is an algebraic variety with a map to $\mathbb{P}^1$. Once we delete the elements of the pencil of curves which meet a crossing point among the four lines, in general six elements, the result is a bundle of elliptic curves over $\mathbb{P}^1$ with at most six points deleted. In this case there is no need to twist by an element of H^1 as this bundle of elliptic curves does have a section.

The finite group G is trivial in this case, and the period map which we'll call γ is related to the *classical* λ function for the upper half plane, which we'll denote $\lambda_{\mathbb{H}}$, by the rule of the cross-ratio

$$\gamma(\lambda(\tau)) = \frac{(e_3(\lambda(\tau)) - e_1(\lambda(\tau))(e_2(\lambda(\tau) - e_4(\lambda(\tau))}{(e_2(\lambda(\tau) - e_1(\lambda(\tau))(e_3(\lambda(\tau) - e_4(\lambda(\tau))}.$$

This extends to a quadratic map $\mathbb{P}^1 \to \mathbb{P}^1$ sending the elements of the pencil which meet an intersection point of any two of the four lines to one of $\{0, 1, \infty\}$.

A choice implicitly made by Weierstrass is

$$e_1(\tau) = \frac{\pi^2}{3}(\theta(0, \tau) + \theta(0, 1 + \tau))$$

$$e_2(\tau) = \frac{\pi^2}{3}(-2\theta(0, \tau) + \theta(0, 1 + \tau))$$

$$e_3(\tau) = \frac{\pi^2}{3}(\theta(0,\tau) - 2\theta(0,1+\tau)).$$

Under the automorphism sending e_1, e_2, ∞ to $0, 1, \infty$ the classical λ function of the upper half plane $\mathbb{H}$ sends e_3 to λ. If we also take

$$e_4(\tau) = 0$$

the automorphism sending e_1, e_2, e_4 to $0, 1, \infty$ sends e_3 instead to the period function for our compact elliptic surface, let us call it γ

$$\gamma(\lambda(\tau)) = \frac{(e_3(\tau) - e_1(\tau))e_2(\tau)}{e_3(\tau)(e_2(\tau) - e_1(\tau))}.$$

$$= \frac{2\lambda(\tau) - \lambda(\tau)^2}{2\lambda(\tau) - 1}.$$

The degree-two map $\lambda \mapsto \gamma(\lambda)$ sends the values of λ which parametrize elements of the pencil which meet a crossing point of two of the same lines, which are

$$-1, 0, \frac{1}{2}, 1, 2, \infty,$$

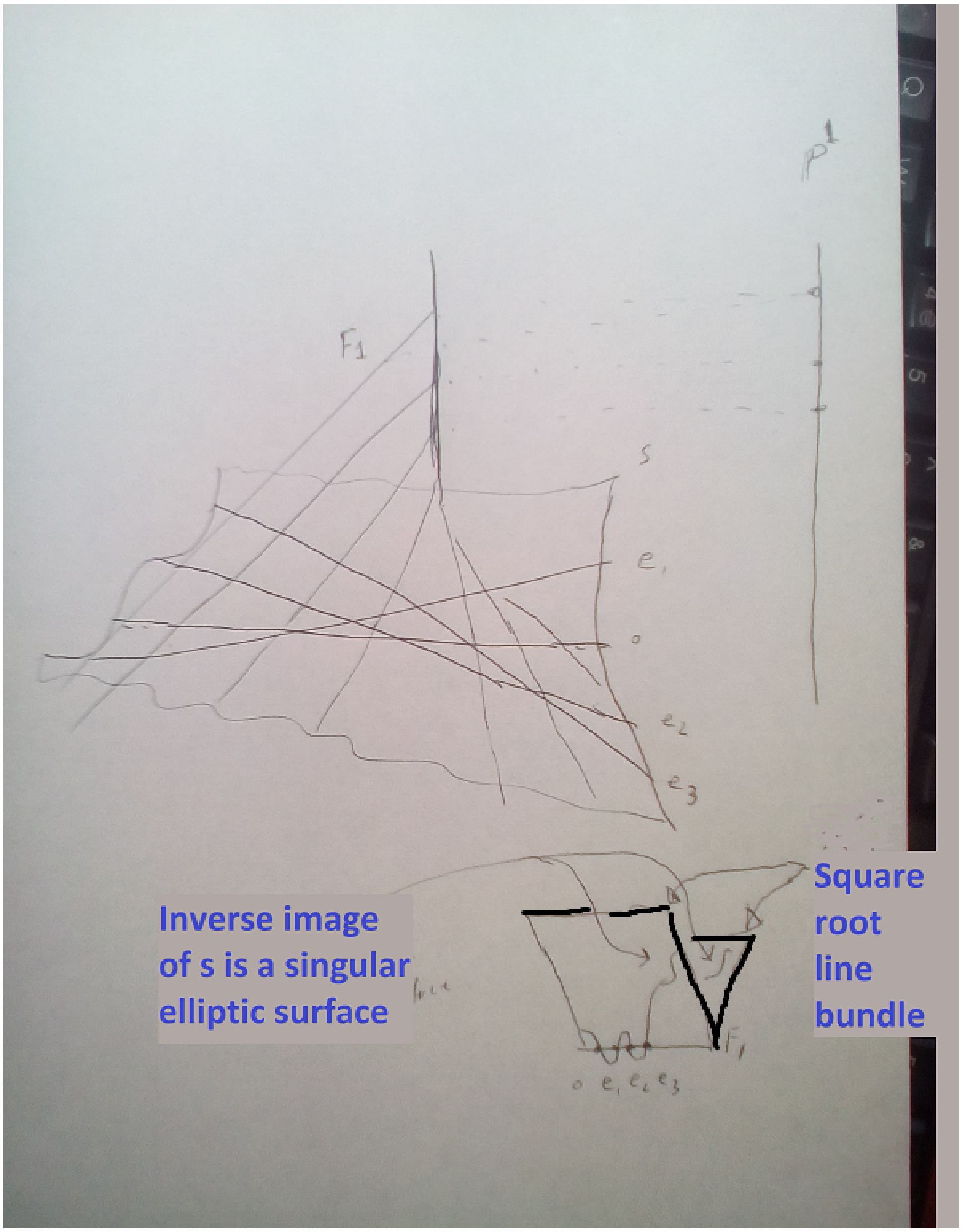
in order, to

$$0, 1, \infty, 0, 1, \infty.$$

The two branching points of the quadratic period map are when $\lambda(\tau) = e^{\pm 2i\pi/6}$, where $\tau = e^{i\pi/2 \mp i\pi/6}$.

The six singular fibers of the resulting compact projective surface have a node each, which is a node in the ambient surface. Once the six nodes are resolved, each singular fiber is a union of two rational curves intersecting at two points each, and each with normal bundle of degree -2.

The unresolved elliptic surface S is the inverse image under tensor square $N \to N^{\otimes 2} \cong L$ of the section image $s(F_1) \subset L$ with L being the line bundle whose section sheaf is dual to the defining ideal $\mathcal{I}$ of the union of four lines in F_1.



P1
F1
s
e1
o
e2
e3
Inverse image of s is a singular elliptic surface
Square root line bundle
F1
o e1 e2 e3

The nontrivial Galois automorphism of the map $\lambda \mapsto \frac{2\lambda-\lambda^2}{2\lambda-1}$ is easily calculated, if we say $\lambda \mapsto c$ then λ satisfies that $2\lambda - \lambda^2 = c(2\lambda - 1)$; the two solutions of this equation add to $2 - 2c$ so the other solution is $\frac{\lambda-2}{2\lambda-1}$.

Rather than preserving the image of the classical lambda function, this automorphism interchanges 0 and 2 and interchanges 1 and -1, and interchanges ∞ and $1/2$. The period map describes a Galois cover of $\mathbb{P}^1$ branched at two points, but it is not possible to lift the Galois automorphism to any automorphism of $\mathbb{H}$ because it sends three interior points to ideal points.

4. Vector fields on bundles of elliptic curves.

Let $S \to M$ be a smooth holomorphic bundle of elliptic curves. Let L be the corresponding line bundle of Lie algebras on M. Let $\mathcal{S}$ be the coherent sheaf on M which consists of fiberwise vector fields on S which commute with addition by local sections of the corresponding Jacobian bundle $J \to M$.

6. Theorem. The sheaf $\mathcal{S}$ is naturally isomorphic with the sheaf of sections of L.

It is useful now to speak of the line bundle M_1 on $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ whose sections correspond to modular forms of weight one. There are two related technicalities, one is that the locally constant structure does not extend to any line bundle on the whole of $\mathbb{P}^1$. A second technicality is that there are no global modular forms of weight one for the subgroup of $Sl_2(\mathbb{Z})$ which is the inverse image of $\Gamma(2) \subset PSl_1(\mathbb{Z})$. Instead, we lift $\Gamma(2)$ isomorphically to the subgroup generated by T^2, ST^2S where $T(\tau) = \tau + 2$, $S(\tau) = -1/\tau$.

We define M_1 to be the vector bundle on $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ whose local sections are modular forms of weight one for $\langle T^2, ST^2S \rangle$. The bundle of Lie algebras corresponding to the universal period map (the identity function of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$) is isomorphic to M_{-1}. One way to see this is to directly construct the line bundle M_k for all k as $\mathbb{C} \times \mathbb{H}$ modulo the action of $\langle T^2, ST^2S \rangle$ where

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} (w, \tau) = ((c\tau + d)^k w, \frac{a\tau + b}{c\tau + d}).$$

For each integer k, and each weakly modular form $f(\tau)$ of weight k, the vector field $f(\tau)\frac{\partial}{\partial w}$ is invariant under the group action. In case $k = -1$ by the identity about lattices in $\mathbb{C}$

$$\mathbb{Z}\frac{a\tau + b}{c\tau + d} \oplus \mathbb{Z} = \frac{1}{c\tau + d}(\mathbb{Z}\tau \oplus \mathbb{Z})$$

we have that the lattices themselves are preserved also, and there results a fiber bundle of elliptic curves covered by M_{-1}, and the corresponding invariant vector field on $\mathbb{C} \times \mathbb{H}$ is $f(\tau)\frac{\partial}{\partial w}$ for any f weakly modular of weight -1.

Two basic periods in the fiber over a point $\lambda(\tau)$ are the complex 'times' it takes for the flow to bring the point 0 to each of $1, \tau$. If we write $f(\tau) = \frac{1}{g(\tau)}$ for g weakly modular of weight 1, these two periods or 'complex times' are

$$g(\tau), \tau g(\tau).$$

Let $S \to \mathbb{P}^1$ be our compactified elliptic surface with six fibers each with two -2 curves. We can construct a fiberwise meromorphic vector field on S with a simple pole on the fiber over one of the branching points of the period map; let's choose the point where $lambda = e^{2\pi i/6}$. Note then $\gamma(\lambda) = e^{-2\pi i/6}$.

We start with a modular form of weight one whose square has a simple zero at the point $\gamma(\lambda)$. The *classical* lambda function takes the value $e^{-2pii/6}$ when $\tau = e^{ipi/2 - i\pi/6}$, and so we take as our modular form

$$f(\tau) = \theta(0, e^{i\pi/2 - i\pi/6})^2 \theta(0, 1+\tau)^2 - \theta(0, 1 + ei\pi/2 - i\pi/6)^2 \theta(0,\tau)^2.$$

The vector field

$$\frac{1}{f(\tau)} \frac{\partial}{\partial w}$$

on $\mathbb{C} \times \mathbb{H}$ is invariant under the action of $\Gamma(2)$ by which $\begin{pmatrix} a & b \\ c & d \end{pmatrix} (w, \tau) = \frac{w}{c\tau+d}, \frac{a\tau+b}{c\tau+d})$, and defines a vector field on the bundle M_{-1} on $\mathbb{P}^1 \setminus \{0, 1, \infty\}$.

If we denote the period map $\mathbb{P}^1 \to \mathbb{P}^1$ by h, then the complement of the singular fibers in our surface S is the total space of $h^* M_{-1}$, and our fiberwise vector field lifts to a vector field having a simple pole on one fiber.

Two basic periods for the elliptic curve over a point $\lambda \in \mathbb{C} \setminus \{0, 1, \infty\} \subset \mathbb{P}^1 \setminus \{0, 1, \infty\}$ are then obtained as follows: starting with λ we evaluate $\gamma(\lambda) = \frac{2\lambda - \lambda^2}{2\lambda - 1}$. Then we define τ to be

$$\tau = \int_0^1 \frac{dz}{\sqrt{z(z-1)(z-\gamma(\lambda))}}.$$

Then our two basic periods are

$$\theta(0, e^{i\pi/2-i\pi/6})^2\theta(0, 1+\tau)^2 - \theta(0, 1+ei\pi/2-i\pi/6)^2\theta(0,\tau)^2$$

and

$$\tau(\theta(0, e^{i\pi/2-i\pi/6})^2\theta(0, 1+\tau)^2 - \theta(0, 1+ei\pi/2-i\pi/6)^2\theta(0,\tau)^2)$$

5. Relation with the Riemann hypothesis.

Now we can interpret $1-\theta(0,1+\tau)^4$ as a rational function on the surface F_1. Each point of M_2 which does not belong to the fiber over $0, 1$, or ∞ is determined by a choice of τ modulo the action of $\Gamma(2)$ and a choice of a constant c, as the value $c\theta(0,\tau)^4$ in the fiber over $\lambda(\tau)$. Denote each such element of $M_2 \subset F_1$ by the symbol $(\lambda(\tau), c\theta(0,1+\tau)^4)$. The rational function corresponding to $1-\theta(0,\tau)^4$ evaluates to

$$1 - c\,\frac{\theta(0,1+\tau)^4}{\theta(0,\tau)^4}$$

this element of $M_2 \subset F_2$.

taking $c = 1$ we see that the restriction of the rational function corresponding to $1-\theta(0,\tau)^4$ to the section value $\theta(0,\tau)^4(\mathbb{P}^1)$ is just the classical lambda function.

That is to say,

7. Principle. The rational function corresponding to the map of importance in the Riemann hypothesis $1-\theta(0,1+\tau)^4 : \mathbb{H} \to \mathbb{C}$, once this corresponding rational function on $\mathbb{F}_1$ is restricted to the section image $\theta(0,\tau)^4(\mathbb{P}^1) \subset F_1$, it equals the restriction to that same section image of the structural map itself $F_1 \to \mathbb{P}^1$.

6. Basic integral calculus.

If $p(t)$ gives a path in a manifold, starting at time 0 (and we may consider time to be a complex holomorphic entity), and if a flow is given on the manifold, whose corresponding operator on functions is the derivation δ, then as long as the path p is an integral curve of the flow, parametrized accordingly, we may explicitly calculate for each complex number c

$$\int_0^c \delta(f)(p(t))dt = \int_0^c \frac{df}{dt}(p(t))dt$$
$$= \int_0^c df(p(t)) = f(p(c)) - f(p(0)).$$

And we can continue the analysis

$$= (e^{c\delta}(f) - f))(p(0)).$$

The element $c\delta$ belongs to the Lie algebra, and knowing how its exponential acts on f allows the calculation of the original integral of the real valued function of t.

A variant of this analysis is the following:

$$\int_0^c \frac{df(p(t))}{\delta(f)(p(t))} = \int_0^c \frac{\delta(f)(p(t))}{\delta(f)(p(t))}dt$$
$$= \int_0^c dt = c.$$

It is this second variant which explains why elliptic integrals calculate periods in the lattice in the Lie algebra. Starting with a one-form of the type $\frac{dz}{g(z)}$ one considers the derivation δ such that $\delta(z) = g(z)$. In other words, so that the function $g(z)$ is the contraction $i_\delta(dz)$ of the one-form dz which is in the numerator. Then one allows the path $p(t)$ to form itself starting from a point $p(0)$, using the exponential formula if one wishes to be explicit; and the integral of $\frac{dz}{g(z)}$ along this particular path has the property that the integral from $p(0)$ to $p(t)$ is just t itself for all values of t.

If $p(c) = p(0)$, the value of c is a period of $\frac{dz}{g(z)}$, and $(e^{c\delta}(g) - g)(p(0)) = 0$.

We can write the one-form related to Riemann's hypothesis as $\frac{d\frac{\lambda}{q}}{\frac{\lambda\tau^{1-s}}{q}}$ and so we can try to choose δ such that

$$\delta(\frac{\lambda}{q}) = \frac{\lambda\tau^{1-s}}{q}.$$

Then starting with any point $p(0)$ we can let $p(t)$ be defined according to the flow of δ, and we will be ensured that the integral of our one-form along the path p from $t = 0$ to $t = c$ will be just c itself.

The paths where $c = 0$ are just paths which lift to a closed path in the Lie algebra; these homotopically trivial since the lifted path is homotopically trivial. In the elliptic curve case we've been just slightly uncareful in analyzing $g(z)$ as if it were a well-defined function, but the point is, it is a well-defined function *on the elliptic surface* and the only genuine difficulty is constructing the vector field. This exists away from the six singular fibers, and the only issue is the compactification.

The question at this juncture is to what extent the same elliptic surface will allow us to unwind the complexity hidden in the expression $log(\frac{\lambda}{q}) = log(\lambda) - i\pi\tau$. And what is the nature of the new vector field δ. Fixing s with $0 < Re(s) < 1$, we know that as a point flowing under δ follows a homotopically nontrivial path, starting from the ideal point 0 in $\mathbb{H}$, the corresponding path integral of our one-form can never reach $i\infty$ if $\zeta(s) = 0$. We do not require time to flow in any particular way, a path in $\mathbb{C}$ starting at 0 is allowed to be arbitrary, and it is allowed to be a closed path except then the image is always homotopically trivial. These observations are quite trivial, the image of the path in $\mathbb{P}^1$ is not even a closed path, it goes from 1 to 0. So we know unconditionally that the integral curve starting at $1 \in \mathbb{P}^1$ does not reach $0 \in \mathbb{P}^1$ if $\zeta(s) = 0$.