A Concrete Approach to Elliptic Integrals

Anil Venkatesh
Elliptic Curves Seminar, Fall 2009

28 September 2009

1 Introduction

Last time, elliptic curves were introduced in the context of finding rational solutions to polynomial equations of the form

\[ y^2 = x^3 + Ax + B \]

In an algebraic context, we looked at the group structure on the elliptic curve \( E \) defined by this equation, which allows for the construction of new rational points from a few initial ones. In terms of analytic properties, we saw that elliptic curves have genus 1; i.e. they are topologically tori, which take the form \( \mathbb{C}/\Lambda \) for some lattice \( \Lambda \). Furthermore, we saw how to use the Weierstrass \( \wp \)-function to construct an explicit map from \( \mathbb{C}/\Lambda \) to \( E(\mathbb{C}) \).

I’m going to speak more to the analytic side of elliptic curves today, in demonstrating how to evaluate an elliptic integral over a closed curve \( \gamma \subset \mathbb{C} \), such as the following.

\[
\int_{\gamma} \frac{dx}{\sqrt{(x-a)(x-b)(x-c)}}
\]

In particular, we’ll examine the case where \( a, b, c \in \mathbb{R} \). We will assume \( a < b < c \) since this condition makes \( y^2 = (x-a)(x-b)(x-c) \) a smooth elliptic curve.

2 Background

Before dealing with the elliptic integral above, I’d like to spend a moment on a more familiar object, the “conic” integral. By this I refer to integrals such as

\[
\int \frac{dx}{\sqrt{1-x^2}}
\]

which in this case gives the arc-length of the unit circle. The process of identifying elliptic curves and tori can be applied instructively to conics, since integrals of the latter sort are well understood. I will therefore take a moment to review the principles of this process for elliptic curves, so as to cast the otherwise mundane conic integration in a new light. From now on, \( E \) will be the elliptic curve defined by \( y^2 = (x-a)(x-b)(x-c) \).
Let us recall the construction of the elliptic integral map

\[ F : E(\mathbb{C}) \to \mathbb{C}/\Lambda \]
\[ F : P \mapsto \int_0^P \frac{dx}{\sqrt{(x-a)(x-b)(x-c)}} \pmod{\Lambda}. \]

We note that the differential form \( \omega = \frac{dx}{y} \) is holomorphic on \( E(\mathbb{C}) \subset \mathbb{C}P^2 \). This follows from the observation that \( \omega \) is certainly holomorphic for nonzero \( y \in \mathbb{C} \), and that the implicit function theorem allows us to express \( \omega \) as a holomorphic form in terms of \( dy \) in a neighborhood of the roots \( x = a, b, c \). One must also verify that \( \omega \) is holomorphic at \([0, 1, 0]\), the intersection of \( E(\mathbb{C}) \) with the line at infinity in \( \mathbb{C}P^2 \), which follows in a similar fashion.

Then the map

\[ E(\mathbb{C}) \to \mathbb{P}^1 \]
\[ (x, y) \mapsto x \]

is a double cover ramified at \( x = a, b, c, \infty \), which arises from the fact that the square root function \( \sqrt{z} \) is not single-valued, except at \( z = 0 \). Therefore, \( \int_\gamma \omega \) is not path-independent for a path \( \gamma \subset \mathbb{P}^1 \) [Sil]. By making branch cuts between pairs of roots, we can produce two single-valued branches of the square root, each a copy of \( \mathbb{P}^1 \). Gluing the copies together along the branch cuts results in the expected torus. We obtain the two periods \( \omega_1, \omega_2 \) of \( E \) by integrating \( \frac{dx}{y} \) around the two non-contractible loops. It can be shown that \( \omega_1 \) and \( \omega_2 \) are linearly independent [Sil], which allows any elliptic integral over a closed loop in \( \mathbb{C}/\Lambda \) to be defined as some integral linear combination of \( \omega_1 \) and \( \omega_2 \) depending on what the loop encloses.

Returning once more to the conic \( C : y^2 = 1 - x^2 \), we begin with the differential form \( \omega = \frac{dx}{y} \). Analogously to the argument above, \( \omega \) is holomorphic for \( y = 0 \); however the form fails to be holomorphic at the intersection points \([1, \pm i, 0]\) of \( C(\mathbb{C}) \) and the line at infinity in \( \mathbb{C}P^2 \), where it has simple poles. Therefore, we will now consider \( C(\mathbb{C}) \) without these two points, for the purposes of integrating \( \omega \).

Proceeding as before, we construct the double covering

\[ C(\mathbb{C}) \setminus \{[1, \pm i, 0]\} \to \mathbb{P}^1 \setminus \{[1, 0]\} \]
\[ (x, y) \mapsto x \]

which is ramified now only at \( x = -1, 1 \). The point at infinity, \([1, 0] \in \mathbb{P}^1 \), is precisely the image of \([1, \pm i, 0]\), which we had discarded. Therefore, we have actually constructed a double covering \( C(\mathbb{C}) \setminus \{[1, \pm i, 0]\} \to \mathbb{C} \), since \( \mathbb{C} \cup \{\infty\} = \mathbb{P}^1 \). Performing a branch cut and gluing the two single-valued branches together, we conclude (perhaps unsurprisingly) that we have identified \( C(\mathbb{C}) \) with a cylinder \( \mathbb{C}/\omega \mathbb{Z} \). To find \( \omega \), we can use standard integration techniques; in this case, \( \omega = 2(\sin^{-1}(1) - \sin^{-1}(-1)) = 2\pi \).

Thus, we can define a conic integral over a closed loop in \( \mathbb{C}/\omega \mathbb{Z} \) as a scalar multiple of \( \omega \) depending on what the loop encloses.
3 Theory of Evaluation

Let us now take the elliptic curve $E : y^2 = (x - a)(x - b)(x - c)$ for real $a < b < c$. Then the corresponding periods are defined as follows.

$$\omega_1 = 2 \int_a^b \frac{dx}{\sqrt{(x-a)(x-b)(x-c)}} \quad \text{and} \quad \omega_2 = 2 \int_b^c \frac{dx}{\sqrt{(x-a)(x-b)(x-c)}}.$$

Note that this condition on the roots of $E$ gives $\omega_1 \in \mathbb{R}$ and $\omega_2 \in i\mathbb{R}$; in particular, the two periods are certainly linearly independent.

Lemma: If $r \leq s$ are real, then the sequence

$$(r_0, s_0) = (r, s), \quad (r_{n+1}, s_{n+1}) = (\sqrt{r_n s_n}, \frac{r_n + s_n}{2})$$

converges and $\lim r_n = \lim s_n$. This limit, denoted by $M(r, s)$, is called the Gauss arithmetic-geometric mean or $r$ and $s$.

Proof: By the Arithmetic-Geometric Mean inequality, it is clear that

$$r_0 \leq r_1 \leq \cdots \leq s_1 \leq s_0.$$

Furthermore,

$$(s_n - r_n) - 2(s_{n+1} - r_{n+1}) = (s_n - r_n) - (s_n - r_n - 2\sqrt{r_n s_n}) = 2\sqrt{r_n s_n} \geq 0$$

so $|s_{n+1} - r_{n+1}| \leq \frac{1}{2}|s_n - r_n|$. Convergence follows [Kna].

The reason for introducing such a cryptic lemma is that we wish to write the integrals for $\omega_1$ and $\omega_2$ in terms of two real parameters, $r < s$, and subsequently show that the integrals are invariant under the iterative averaging process above. Since that process has a limit, we will then be able to evaluate the integrals exactly.

Under the change of variables $\sqrt{x - a} = \sqrt{b - a} \sin \theta$ and $\sqrt{x - b} = \sqrt{c - b} \cos \theta'$, we obtain

$$\omega_1 = 2 \int_0^{\frac{\pi}{2}} \frac{d\theta}{\sqrt{(c-b) \sin^2 \theta + (c-a) \cos^2 \theta}}$$

$$\omega_2 = 2i \int_0^{\frac{\pi}{2}} \frac{d\theta'}{\sqrt{(b-a) \sin^2 \theta' + (c-a) \cos^2 \theta'}}.$$

Observe that we can write these integrals as $\omega_1 = 2I(\sqrt{c-b}, \sqrt{c-a})$ and $\omega_2 = 2iI(\sqrt{b-a}, \sqrt{c-a})$ where we define $I(r, s)$ for $r < s$ by

$$I(r, s) = \int_0^{\frac{\pi}{2}} \frac{d\theta}{\sqrt{r^2 \sin^2 \theta + s^2 \cos^2 \theta}}.$$

It now remains to be shown that $I(r, s) = I(\sqrt{rs}, \frac{s+r}{2})$, implying that $I(r, s) = I(M(r, s), M(r, s)) = \frac{\pi}{2M(r, s)}$. We apply a second change of variables,

$$\sin \theta = \frac{2s \sin \varphi}{(s + r) + (s - r) \sin^2 \varphi}, \quad 0 \leq \varphi \leq \frac{\pi}{2}.$$
and obtain

\[ I(r, s) = \int_0^{\frac{\pi}{2}} \frac{d\varphi}{\sqrt{rs \sin^2 \varphi + \left(\frac{s+r}{2}\right)^2 \cos^2 \varphi}} = I\left(\sqrt{rs}, \frac{r+s}{2}\right). \]

Therefore, \( I(r, s) = \frac{\pi}{2M(r, s)} \). \[\text{[Kna]}\]

4 Example

Let us consider the elliptic curve \( E : y^2 = (x+3)(x+1)(x-1) \) and the path \( \gamma : |x| = 2 \), with counter-clockwise orientation and positive square-root determination. Then

\[ \int_{\gamma} \omega = 2 \int_{b}^{c} \omega = \omega_2 \]

by our previous calculations. In this case,

\[ \omega_2 = 2iI\left(\sqrt{1-(-1)}, \sqrt{1-(-3)}\right) = \frac{\pi i}{2M(\sqrt{2}, 2)} = \frac{\pi i}{2 \times 1.69443} = 0.92704i. \]

References
