Introduction to abelian varieties and the Mumford–Tate conjecture

From Kepler's laws to number theory

J. M. Commelin, *the 13th of October, 2016*

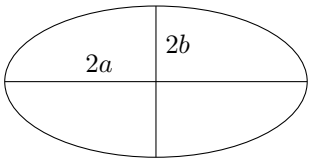
The subtitle might suggest that the following exposition provides a continuous—maybe even smooth—path from physics to number theory. Alas! If any such hope was aroused; I will now correct it immediately. The prelude consists of a medley of ellipses, integrals, complex analysis, and historical intermezzos. Then follows a sharp cut, and the theme changes to number theory. It is not farfetched to say that we compose a canon on a hidden motif, a counterpoint, involving Hodge theory and Galois theory.

Prelude

Kepler discovered that the classical Platonic idea was wrong: the orbits of planets around the sun are not circles but ellipses! The sun is located precisely in one of the two focal points of such an elliptical orbit. There are a couple of questions that we may ask about such ellipses.

- What is the area enclosed by the ellipse?
- What is the length of the ellipse/orbit?
- What is the period of the planet?
- What is the posiotion of the planet at time t?
- What is the speed of the planet at time t?

Answers to some of these questions are easy, and others are hard. For example, the area of an ellipse is $4ab \cdot \pi$, where a, and b are the semi-axes of the ellipse.



$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$$

However, the arc length turns out to be very hard. In general, it is given by the integral

$$\int_{x_0}^{x_1} \sqrt{1 + f'(x)^2}\mathrm{d}x;$$

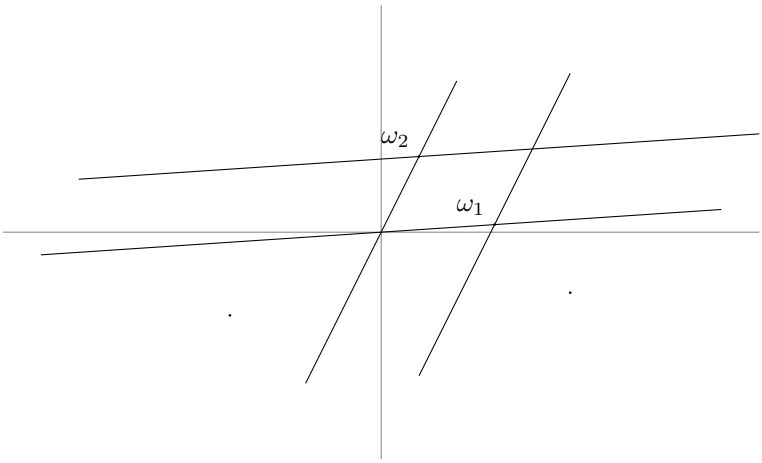
where f is a funtion of which the arc is the graph. In our case, for arcs above the x-axis, we have $y = f(x) = b\sqrt{a^2 - x^2}/a$. After substituting $k = \sqrt{a^2 - b^2}/a$, we find the following integral for the arc length:

$$L_{x_0}^{x_1} = \int_{x_0}^{x_1} \sqrt{\frac{a^2 - k^2x^2}{a^2 - x^2}}\mathrm{d}x$$

Such integrals are aptly named *elliptic integrals*.

To make a long story short: lots of people tried to find exact formulas for these integrals, and they failed. But in the first half of the 19th century, Abel and Jacobi came up with a marvelous idea: Instead of looking at the function $x_1 \mapsto L_{x_0}^{x_1}$, they extended it to a multi-valued complex function, and they looked at its inverse. The resulting function was called an *elliptic function*. As opposed to the elliptic integrals, these elliptic functions are not multi-valued, but proper well-defined (meromorphic) functions: the way we like them nowadays. Eisenstein and Weierstrass also made immense contributions; and in the second half of the

same century, the picture was quite clear. These elliptic functions are doubly periodic; meaning that there are two complex numbers ω_1 and ω_2 such that $\phi(z + m \cdot \omega_1 + n \cdot \omega_2) = \phi(z)$.



So every elliptic function ϕ actually is a function on a torus! The torus in question, $E = \mathbb{C}/(\mathbb{Z} \cdot \omega_1 \oplus \mathbb{Z} \cdot \omega_2)$ is what is called an *elliptic curve*. An important discovery (by Weierstrass) is that there is a special elliptic function on E. This function, usually denoted $\wp$, has the remarkable property that all its derivatives are also elliptic functions, with the same periods. Besides that, $\wp$ and $\wp'$ satisfy the equation

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3,$$

where g_2 and g_3 are complex numbers that only depend on ω_1 and ω_2. The poles of $\wp$ are exactly at the points $m\omega_1 + n\omega_2$.

For more information about this wonderful tale, we refer to:

[1] Rice, Adrian; Brown, Ezra. Why ellipses are not elliptic curves. *Math. Mag.* 85 (2012), no. 3, 163–176.

[2] Arnold, V. I. Kepler's second law and the topology of abelian integrals (according to Newton) [Kvant 1987, no. 12, 1721]. *Kvant selecta: algebra and analysis, II*, 131–140, Math. World, 15, *Amer. Math. Soc., Providence*, RI, 1999.

* * * * * * *

Intermezzo: Elliptic curves and abelian varieties over $\mathbb{C}$

Let us recapitulate what we have got so far. An elliptic curve is given by two periods $\omega_1, \omega_2 \in \mathbb{C}$, and we require that ω_1 and ω_2 span $\mathbb{C}$ as real vector space. In other words: $\omega_1/\omega_2 \notin \mathbb{R}$. The elements ω_1 and ω_2 generate an abelian group Λ, and the elliptic curve is the torus $E = \mathbb{C}/\Lambda$.

On the other hand, by Weierstrass's observation, we can define a map

$$E \to \mathbb{C} \times \mathbb{C}, \qquad (z + \Lambda) \mapsto (\wp(z), \wp'(z)).$$

This map is well-defined, except when $\wp$ or $\wp'$ has a pole; and this map is injective! In conclusion, (almost all) the points on E can be described as the subset of points in $\mathbb{C} \times \mathbb{C}$ that satisfy an equation of the form

$$Y^2 = X^3 + aX + b.$$

(Remark: not all pairs (a, b) occur: the resulting curve must be smooth. This means that the discriminant $-16(4a^3 + 27b^2)$ should not vanish.)

We can now generalise this to higher dimensions. A complex torus of dimension g is the space V/Λ, where $V \cong \mathbb{C}^g$, and $\Lambda \cong \mathbb{Z}^{2g}$ is a subgroup of V that spans V as real vector space. Such a complex torus is called an *abelian variety* if there is a meromorphic map $V/\Lambda \to \mathbb{C}^N$, such that the image is an algebraic subset: the solution set to a several polynomial relations. In contrast to elliptic curves, not every complex torus of dimension ≥ 2 satisfies this condition. So there are complex tori that are not abelian varieties.

An amazing feature of elliptic curves and abelian varieties is that they have a group structure. This is a pretty straight-forward corollary of the definition: after all V/Λ is a quotient group. However, what is absolutely unclear is that the multiplication and inversion are also given by polynomial maps. In other words, if (x, y) and (w, z) in $\mathbb{C}^2$ are points on an elliptic curve given by $Y^2 = X^3 + aX + b$; then the coordinates of $(x, y) \oplus (w, z)$ are polynomial expressions in x, y, w, and z. Alas, there is no time to go into the details of this marvellous property.

Aria: Mumford–Tate groups

We attach a group to every abelian variety. Let $A = V/\Lambda$ be an abelian variety of dimension g. Note that $\mathbb{C}^\star$ acts canonically on V; after all $\mathbb{C}^\star \subset \mathrm{GL}(V)$. The Mumford–Tate group is an algebraic subgroup of $\mathrm{GL}(\Lambda)$.

> *Aside:* What is an algebraic subgroup? Recall that $\Lambda \cong \mathbb{Z}^{2g}$; and therefore $\mathrm{GL}(\Lambda) \cong \mathrm{GL}_{2g}(\mathbb{Z})$. An algebraic subgroup of $\mathrm{GL}_{2g}(\mathbb{Z})$ is a subgroup $H \subset \mathrm{GL}_{2g}(\mathbb{Z})$ that is also an algebraic subset. In other words, there must be certain polynomials in the matrix coefficients of $2g \times 2g$-matrices, such that H is precisely the solution set of those polynomials. Examples: SL_{2g} ($\det(M) = 1$) or O_{2g} ($MM^t = I$).

The Mumford–Tate group of A is the smallest subgroup of $\mathrm{GL}(\Lambda)$ such that the subgroup of $\mathrm{GL}(\Lambda \otimes \mathbb{R}) = \mathrm{GL}(V)$ defined by the same polynomials contains the image of $\mathbb{C}^\star$.

We should not be surprised that the Mumford–Tate group can become quite big. After all, $\Lambda \subset V$ is not the naive embedding; the subgroup $\Lambda \subset V$ is embedded in a "twisted" way. For example, in the picture above, $\Lambda \subset \mathbb{C}$ was not embedded as $\mathbb{Z}[i]$.

We will denote the Mumford–Tate group of A with $\mathrm{G}_{\mathrm{MT}}(A)$.

Intermezzo: Elliptic curves and abelian varieties over $\mathbb{Q}$

Let E be an elliptic curve, defined by an equation $Y^2 = X^3 + aX + b$. If the coefficients a and b lie in $\mathbb{Q}$, then we say that E is defined over $\mathbb{Q}$. Similarly, if an abelian variety is the solution set of polynomials with rational coefficients, then it is defined over $\mathbb{Q}$.

We have to be slightly imprecise about what we mean with an abelian variety over $\mathbb{Q}$. But in what follows, we will consider an abelian variety over $\mathbb{C}$, together with polynomials that describe it as algebraic subset. And we assume that these polynomials have coefficients in $\mathbb{Q}$. (For another choice of polynomials, this might not be true. So we treat the polynomials as part of the data.)

Aria: Galois groups

We denote with $\bar{\mathbb{Q}}$ the subset of $\mathbb{C}$ consisting of all complex numbers that are the root of a polynomial with coefficients in $\mathbb{Q}$. It turns out that $\bar{\mathbb{Q}}$ is a field. The central player in this intermezzo is the group of automorphisms $\bar{\mathbb{Q}} \to \bar{\mathbb{Q}}$, which we denote with $\Gamma = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

The key point is that Γ acts on a special subset of A: it preserves torsion points. To get an idea for why this is true, assume that A has dimension 1; that is, assume that A is an elliptic curve. Let $P = (x, y) \in A$ be a torsion point: there is some number n such that $n \cdot P = 0$ in A. We claim that $x, y \in \bar{\mathbb{Q}}$. Indeed, the addition on A is defined via polynomials, and therefore multiplication by n is given by polynomials. After applying these polynomials to x and y, we end up with elements of $\mathbb{Q}$, which proves our claim that $x, y \in \bar{\mathbb{Q}}$.

Intermezzo: Profinite integers and Tate modules

If n is an integer, and m is a divisor of n, then there is a natural ring homomorphism

$$\phi_{n,m}\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}, \qquad (x \mod n) \mapsto (x \mod m).$$

We let $\hat{\mathbb{Z}}$ denote the set of infinite sequences $(\dots, a_n, \dots, a_2, a_1)$, with $a_n \in \mathbb{Z}/n\mathbb{Z}$, that satisfy the following property: for all positive integers n, divisible by a positive integer m we have $\phi_{n,m}(a_n) = a_m$. By pointwise addition and multiplication, the set $\hat{\mathbb{Z}}$ acquires a ring structure, and $\mathbb{Z}$ is in a natural way a subring of $\hat{\mathbb{Z}}$. The ring $\hat{\mathbb{Z}}$ is called the ring of *profinite integers*.

Now, we do a similar thing with the torsion points of A. Let us denote the subgroup of n-torsion points by $A[n]$. If g denotes the dimension of A, then $A[n]$ is a free module of rank $2g$ over $\mathbb{Z}/n\mathbb{Z}$. Let m be a divisor of n. Then $n = m \cdot q$, and multiplication by q gives a map

$$A[n] \to A[m], \qquad x \mapsto q \cdot x.$$

We can put these torsion points into infinite sequences as well. Let $T(A)$ be the set of infinite sequences $(\dots, x_n, \dots, x_2, x_1)$, with $x_n \in A[n]$, that satisfy the following property: for all positive integers n, divisible by a positive integer m we have $q \cdot x_n = x_m$, where $q = n/m$. By pointwise addition the set $T(A)$ acquires a group structure, and by pointwise addition with elements of $\hat{\mathbb{Z}}$, the group $T(A)$ is naturally endowed with a $\hat{\mathbb{Z}}$-module structure. It is a module that is free of rank $2g$. We call $T(A)$ the *Tate module* of A. (Remark: In the literature, the Tate module usually means something slightly different.)

Canon: The Mumford–Tate conjecture

Now it is time to put 1 and 1 together; to make 2. Recall from the aria on Mumford–Tate groups that we defined an algebraic subgroup $\mathrm{G_{MT}}(A) \subset \mathrm{GL}(\Lambda)$. We defined it as the smallest subgroup satisfying some condition, namely: it is the solution set of certain polynomials, and the solution set of those polynomials in $\mathrm{GL}(\Lambda \otimes R) = \mathrm{GL}(V)$ has to contain the image of $\mathbb{C}^* \subset \mathrm{GL}(V)$.

By the aria on Galois groups, we know that $\Gamma = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts on the torsion points of A. It preserves the sets $A[n]$, for all n; and therefore Γ acts on $T(A)$. The action of Γ on $T(A)$ is $\hat{\mathbb{Z}}$-linear. Analogous to the definition of $\mathrm{G_{MT}}(A)$, we define $\mathrm{G_T}(A)$ to be the smallest algebraic subgroup of $\mathrm{GL}(T(A)) \cong \mathrm{GL}_{2g}(\hat{\mathbb{Z}})$ that contains the image of Γ.

Now the canon truly starts, and the two melodies intertwine. A fantastic theorem says that there is a natural map $\Lambda \to T(A)$. Via this map, the polynomials that define $\mathrm{G_{MT}}(A) \subset \mathrm{GL}(\Lambda)$ also define an algebraic subgroup of $\mathrm{GL}(T(A))$. The Mumford–Tate conjecture asserts that this subgroup is precisely $\mathrm{G_T}(A)$.

Serre showed that this conjecture is true for elliptic curves, even before the conjecture was first stated. Mumford and Tate were inspired by the result of Serre, and put forward this conjecture. There has been a lot of work on this conjecture; and it is not possible to sum up all the known cases, or to give credit to everyone who contributed. Still we want to give an indication of the state of the art: The Mumford–Tate conjecture is known for abelian varieties of dimension $g \leq 3$, or if the dimension is a prime number, and the abelian variety can not be written as a product of lower-dimensional abelian varieties. In general, the conjecture is wide open.

* * * * * * *

This is the end of a short musical expedition into the world of abelian varieties. I thank you for your attention.