Elliptic Curves and Modular Forms

Jerome William Hoffman

October 19, 2013

Abstract

This is an exposition of some of the main features of the theory of elliptic curves and modular forms.

1 Elliptic Curves

1.1 What they are.

References: [3], [6], [8], [9], [11].

Definition 1.1. Let K be a field. An elliptic curve over K is a pair (E, O) where E is a nonsingular projective algebraic curve defined over K and $O \in E(K)$ is a K - rational point such that there is a morphism

$$E \times E \longrightarrow E$$

of algebraic varieties defined over K making E into a group with O as the identity element of the group law.

It turns out:

1. That E is a *projective* variety forces the group law to be commutative.
2. E necessarily has genus 1. Conversely any nonsingular (smooth) projective curve E of genus 1 with a K - rational point O becomes a commutative algebraic group with O as origin in a unique way.

Note that the existence of a rational point is essential (if K is algebraically closed there will always be rational points, but not in general). Another way of saying this is that an elliptic curve is an abelian variety of dimension one.

It is a theorem that every elliptic curve is isomorphic with a cubic in the projective plane $\mathbf{P}^2$, $F(X,\ Y,\ Z) = 0$, in such a way that O becomes an

inflection point (one of the 9 inflection points). Nonsingularity is expressed by saying that the equations

$$\partial F/\partial X \ = \ \partial F/\partial Y \ = \ \partial F/\partial Z \ = 0$$

have only the solution $(0,0,0)$ in the algebraic closure $\overline{K}$ (This is the condition for char $(K) \neq 3$. In characteristic three one must add the condition $F(X,\ Y,\ Z) = 0$). In this model of an elliptic curve the group law takes on an especially simple form:

$$P \ + \ Q \ + \ R \ = \ O \ \Leftrightarrow \ P,\ Q,\ R \text{ are } \text{ collinear.}$$

We can always find a generalized Weierstrass model in the shape:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

In fact, if $\text{char}(K) \neq 2, 3$ one can always find a model of E as a plane cubic of the form

$$y^2 \ = \ 4x^3 - Ax - B, \quad A,\ B \in K.$$

The nonsingularity is equivalent to the nonvanishing of the discriminant

$$\Delta \ = \ A^3 - 27B^2 \neq 0.$$

The origin has become the unique point at infinity on this curve. Namely setting $x = X/Z,\ y = Y/Z$ we get a homogeneous cubic

$$F(X,\ Y,\ Z) \ = \ Y^2Z \ - \ (4X^3 - AXZ^2 - BZ^3) = 0$$

and $O = (0, 1, 0)$. One can give explicit formulas for the group law as follows: First notice that the the lines through O are precisely the vertical lines in the $(x,\ y)$ - plane. Therefore the group law gives $P + (-P) + O = O \Leftrightarrow P, -P, O$ are collinear $\Leftrightarrow P, -P$ lie on the same vertical line. This shows that

$$(x(-P),\ y(-P)) \ = \ (x(P),\ -y(P)).$$

To add two points, let $(x_1,\ y_1) = (x(P_1),\ y(P_1))$, $(x_2,\ y_2) = (x(P_2),\ y(P_2))$. The straight line connecting P_1 and P_2 meets E in a third point, which is $P_3 = -(P_1 + P_2)$ according to the definition of the group law. Therefore, by what we have seen

$$(x(P_1 + P_2),\ y(P_1 + P_2)) \ = \ (x(P_3),\ -y(P_3)).$$

We find the coordinates $(x_3,\ y_3) = (x(P_3),\ y(P_3))$. The line connecting P_1 and P_2 is

$$y = m(x - x_1) + y_1, \quad m = \frac{y_2 - y_1}{x_2 - x_1}$$

Putting this into the equation $y^2 - (4x^3 - Ax - B) = 0$ we get a cubic polynomial $f(x) = 0$ whose roots are the x - coordinates of the intersection of this line with E. Explicitly

$$f(x) = -4x^3 + m^2x^2 + (A - 2m^2x_1 + 2my_1)x + (B - 2mx_1y_1 + m^2x_1^2 + y_1^2)$$

We have $f(x) = -4(x - x_1)(x - x_2)(x - x_3)$; therefore expanding and comparing the quadratic terms we obtain $x_1 + x_2 + x_3 = m^2/4$. Thus

$$\begin{aligned} x(P_1 + P_2) &= \frac{(y_1 - y_2)^2 - 4(x_1 + x_2)(x_1 - x_2)^2}{4(x_1 - x_2)^2} \\ &= \frac{-2B - A(x_1 + x_2) + 4x_1x_2(x_1 + x_2) - 2y_1y_2}{4(x_1 - x_2)^2} \\ y(P_1 + P_2) &= -\left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x(P_1 + P_2) - x_1) - y_1 \end{aligned}$$

These formulas are valid only if $x_1 \neq x_2$. If $x_1 = x_2$, then $y_1 = \pm y_2$. If $y_1 = -y_2$ then these points are opposite one another: $P_1 + P_2 = O$. If $y_1 = y_2 \neq 0$ ie., $P_1 = P_2$, then repeat the above calculation but instead of the line connecting P_1 and P_2, take the tangent line at $P_1 = P_2$, whose slope is found as in elementary calculus:

$$m = \frac{12x_1^2 - A}{2y_1}$$

For example, the point $P = (2, 5)$ is on the curve $E : y^2 = x^3 + 17$. One computes

$$\begin{aligned} P &= (2, 5) \\ 2P &= (-64/25, 59/125) \\ 3P &= (5023/3249, -842480/185193) \\ 4P &= (38194304/87025, -236046706033/25672375) \\ 5P &= (279124379042/111229587121, 212464088270704525/37096290830311831) \end{aligned}$$

One see that the "size" of the point grows quite rapidly. Size is measured by an invariant called the height of a point. The point P is of infinite

order on this curve. The rank the finitely generated abelian group $E(\mathbf{Q})$ is 1 (see the discussion of elliptic curves over number fields in section 1.4. One computes that $\Delta_E = -2^4 3^3 17^2$, and $j_E = 0$. This means that one can reduce E modulo the prime p and obtain an elliptic curve over the finite field $\mathbf{F}_p$ for all $p \neq 2, 3, 17$ (the curve becomes singular at these primes). See the discussion of elliptic curves over finite fields in section 1.6.

Here is another example: $E : y^2 + y = x^3 - x^2$. One computes: $\Delta_E = -11$, and $j_E = -2^{12}/11$. The point $P = (1, 0)$ is on the curve, and one finds:

$$\begin{aligned} P &= (1,0) \\ 2P &= (0,0) \\ 3P &= (0,-1) \\ 4P &= (1,-1) \\ 5P &= \infty. \end{aligned}$$

Therefore this is an element of order 5 in the group. One can show $E(\mathbf{Q}) = \mathbf{Z}/5$.

Today there are software packages that will compute many things about elliptic curves and modular forms. Some of the computations in this paper were done in a Sage worksheet, using pari/gp and Magma. We also used Mathematica.

Although elliptic curves can be put into the standard form, it is not always the case that they arise this way. For example, an equation of the form $y^2 = P(x)$, where $P(x)$ is a quartic polynomial can define an elliptic curve if the roots of $P(x)$ are distinct. This curve will have singular points on the line at infinity in the projective plane so that the elliptic curve is the nonsingular model of this curve. Also, one must have at least one K - rational point on this. Another way to construct elliptic curves is to take the transversal intersection of two quadric surfaces in projective 3 - space $\mathbf{P}^3$.

Example: We can put the Fermat curve $x^3 + y^3 = 1$ into Weierstrass form by the substitution

$$u = 9(1 + x)/(1 - x), \qquad v = 3y/(1 - x)$$

which leads to an equation $u^2 = 4v^3 - 27$.

1.2 History

A brief digression on the history of this. The group law on a cubic seems a mysterious thing the first time one encounters it, but in fact it arose

in a natural way in attempting to generalize the addition formula for the trigonometric functions. The circle $Z: \ x^2 + y^2 = 1$, which is a curve of genus 0, carries a natural group structure gotten from the parametrization $x = \cos(z), y = \sin(z)$. Let $(x_1, \ y_1) = (\cos(z_1), \ \sin(z_1))$ and $(x_2, \ y_2) = (\cos(z_2), \ \sin(z_2))$. Then if

$$(x_3, \ y_3) = (\cos(z_1 + z_2), \ \sin(z_1 + z_2))$$

we get from the addition laws for the sine and cosine:

$$\begin{aligned} x_3 &= x_1x_2 - y_1y_2 \\ y_3 &= x_1y_2 + y_1x_2 \end{aligned}$$

The group law is that of the parameter z under addition, and by the periodicity of the trigonometric functions, the z may be taken modulo 2π. This parametrization gives an isomorphism of complex points

$$\mathbf{C}/2\pi\mathbf{Z} \simeq \ Z(\mathbf{C}) \simeq \ \mathbf{C}^\times$$

The group law can be expressed in the form

$$\int_0^{y_1} \frac{dx}{\sqrt{1-x^2}} + \int_0^{y_2} \frac{dx}{\sqrt{1-x^2}} \ = \ \int_0^{x_1y_2+y_1x_2} \frac{dx}{\sqrt{1-x^2}}$$

for the integral defining the arcsin function. It was in this form that Euler, expanding on earlier special cases treated by Fagnano, found the group law on curves of genus 1 in the form

$$\int_0^{(x_1,y_1)} \frac{dx}{\sqrt{P(x)}} + \int_0^{(x_2,y_2)} \frac{dx}{\sqrt{P(x)}} \ = \ \int_0^{(x_3,y_3)} \frac{dx}{\sqrt{P(x)}}$$

where $P(x)$ is a cubic or quartic polynomial, and

$$(x_3, \ y_3) \ = \ (R(x_1, y_1, x_2, y_2), \ S(x_1, y_1, x_2, y_2))$$

for *rational functions*, ie., quotients of polynomials, R, S. Such integrals became known as elliptic integrals (because these arise when you compute the arclength of an ellipse). The differential form

$$\omega \ = \ \frac{dx}{\sqrt{P(x)}}$$

is the essentially unique everywhere holomorphic differential 1 - form on the curve. It is also the essentially unique differential form invariant under the

translations of the group. Later, Abel and Jacobi defined the analogues $\varphi(z)$ of the trig functions by setting

$$z = \int_0^{\varphi(z)} \frac{dx}{\sqrt{P(x)}}$$

and these satisfy addition laws analogous to those of the trig functions. Moreover they have a periodicity property, like the trig functions. Here it is necessary to regard $\varphi(z)$ as a function of a complex variable z. Then there are *two* independent periods:

$$\varphi(z + m\omega_1 + n\omega_2) \;=\; \varphi(z)$$

for all $m, n \in \mathbf{Z}$, where ω_1, ω_2 are complex numbers linearly independent over $\mathbf{R}$, in other words spanning a *lattice* in $\mathbf{C}$. These functions are called elliptic functions. They are meromorphic in z.

These periods have the following interpretation. The manifold of complex points $E(\mathbf{C})$ is a topological surface ("Riemann surface") which looks like the surface of a doughnut. This is one way of seeing that E has genus 1: each closed connected surface is homeomorphic to a 2 - sphere with g handles attached, the integer g being the genus. The homology group is free of rank 2:

$$\mathrm{H}_1(E(\mathbf{C}),\ \mathbf{Z}) \;=\; \mathbf{Z}^2 \;=\; \mathbf{Z}\alpha_1 \oplus \mathbf{Z}\alpha_2$$

with some chosen generators $\alpha_1,\ \alpha_2$. The periods are

$$\omega_1 \;=\; \int_{\alpha_1} \omega, \qquad \omega_2 \;=\; \int_{\alpha_2} \omega$$

The integrals that Euler used to define the group law on a curve of genus 1 are ambiguous in that the paths joining 0 and (x_1, y_1) etc. have not been specified, but any two choices differ by an element of the homology group, and therefore the equations defining the addition law should be understood as congruences modulo the lattice of periods.

Example: The curve $E : y^2 + y = x^3 - x^2$ of discriminant -11 we considered before. In a suitable basis, the period matrix is

$$(6.3460465213977671..., (3.1730232606988...) - (1.4588166169384952...)i).$$

The ratio of these two numbers is

$$\tau = (1.65101556391170559....) + (0.7590643816862466676927...)i$$

which is a point in the upper half plane $\mathbf{H}$. The elliptic curve E is isomorphic over $\mathbf{C}$ to the elliptic curve $\mathbf{C}/L_\tau$ where $L_\tau \subset \mathbf{C}$ is the lattice $\mathbf{Z} + \mathbf{Z}\tau$. See section 1.5.

1.3 Modular families

There is an important difference between the trigonometric and the elliptic case. There is essentially only one class of trigonometric functions, reflecting the fact that there is only one curve of genus 0 (projective, smooth, over an algebraically closed field) namely the projective line $\mathbf{P}^1$. The curves of genus 1 depend on one free parameter. In other words, there are nontrivial families of curves of genus 1. For example, Legendre's family

$$E_\lambda : \ y^2 = x(x-1)(x-\lambda)$$

Jacobi's family

$$E_\kappa : \ y^2 = 1 - 2\kappa x^2 + x^4$$

Hesse's family

$$E_\mu : \ X^3 + Y^3 + Z^3 - 3\mu XYZ = 0$$

The intersection of quadrics E_θ:

$$\begin{aligned} X_1^2 + X_3^2 - 2\theta X_2 X_4 &= 0 \\ X_2^2 + X_4^2 - 2\theta X_1 X_3 &= 0 \end{aligned}$$

Bianchi's family, E_ζ defined as the intersection of the 5 quadrics in $\mathbf{P}^4$:

$$\begin{aligned} Q_0(X) &= X_0^2 + \zeta X_2 X_3 - (1/\zeta) X_1 X_4 = 0 \\ Q_1(X) &= X_1^2 + \zeta X_3 X_4 - (1/\zeta) X_2 X_0 = 0 \\ Q_2(X) &= X_2^2 + \zeta X_4 X_0 - (1/\zeta) X_3 X_1 = 0 \\ Q_3(X) &= X_3^2 + \zeta X_0 X_1 - (1/\zeta) X_4 X_2 = 0 \\ Q_4(X) &= X_4^2 + \zeta X_1 X_2 - (1/\zeta) X_0 X_3 = 0 \end{aligned}$$

In all these examples one has an elliptic curve except at the finitely many values of the respective parameter where the corresponding curve acquires a singular point. The parameters, $\lambda, \kappa, \mu, \theta, \zeta$, are called *moduli*, or more exactly, algebraic moduli. When the base field is that of the complex numbers, it was discovered that these are all expressible as functions of a complex variable τ, with $\mathrm{Im}(\tau) > 0$, eg., $\lambda = \lambda(\tau)$, etc. This τ is called the transcendental modulus. The expressions can be given in the form $f(\tau)/g(\tau)$, for analytic functions $f(\tau)$, $g(\tau)$ with special transformation properties, called *modular forms*.

The study of elliptic curves has very different features over different types of ground fields K. We will mention some of the highlights in the special cases where K is

1. A number field.
2. The complex numbers $\mathbf{C}$.
3. A finite field $\mathbf{F}_q$.
4. A p - adic field.

1.4 Number fields

This is the most difficult one to study. Elliptic curves over $\mathbf{Q}$ were studied in antiquity. Diophantos includes several examples of finding rational points on elliptic curves. These were later examined by Fermat, who discovered the method of infinite descent for establishing the existence or nonexistence of rational points. An excellent reference for this is Weil's [11]. This method of infinite descent became an important part of the theorem proved by Mordell in 1922 and generalized by Weil a few years after:

Theorem 1.1. *Let E be an elliptic curve over a number field K. Then the group of rational points $E(K)$ is a finitely generated abelian group.*

This means $E(K) \simeq \mathbf{Z}^r \oplus F$ for an integer $r \geq 0$ called the rank of E over K, and a finite abelian group F. There are many open questions here. The rank is not an effectively computable integer; in many cases one can find the group of rational points (indeed Fermat did this in some cases), but there is no known general procedure for finding all the points. Let $K = \mathbf{Q}$; one does not know if the rank of an elliptic curve over $\mathbf{Q}$ can be arbitrarily large (the largest known rank is 19). There are deep conjectures (Birch and Swinnerton - Dyer) that connect the rank of E with an invariant called the L - function of E.

Example: The curve $E : y^2 + y = x^3 - 7x + 6$. $\Delta_E = 5077$. One can show that $E(\mathbf{Q}) = \mathbf{Z}^3$. In fact, a set of generators of this group are the points $(1, 0)$, $(2, 0)$, $(0, 2)$. For instance we can add: $(1, 0) + (2, 0) = (-3, -1)$. One way to show that a point has infinite order is to compute its canonical height. For instance, height$(1, 0) = 0.668205165651..$, which is nonzero. That these 3 points are independent in the Mordell-Weil group can be verified by computing the determinant of the height matrix, which is also nonzero: $0.41714355875838396981....$

1.5 Complex numbers

Every elliptic curve over the complex numbers is isomorphic as an abelian group to $E_L = \mathbf{C}/L$ where $L \subset \mathbf{C}$ is a lattice, ie., a free abelian group of

rank 2 whose generators are linearly independent over $\mathbf{R}$. In particular, as a group, $E(\mathbf{C}) = S^1 \times S^1$, a product of circles.

Without loss of generality we can take the lattices generated by 1 and τ, with $\mathrm{Im}(\tau) > 0$,

$$L_\tau \;=\; \mathbf{Z} \oplus \mathbf{Z}\tau, \quad E_\tau = \mathbf{C}/L_\tau.$$

Moreover, one proves that E_τ is isomorphic to $E_{\tau'}$ if and only if

$$\tau' = \frac{a\tau + b}{c\tau + d}, \quad \text{where } \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

is a matrix of integers with determinant $ad - bc = 1$.

The construction is due to Weierstrass. One forms the meromorphic L_τ - periodic function

$$\wp(z;\tau) \;=\; \frac{1}{z^2} \;+\; \sum_{\substack{\omega \in L_\tau \\ \omega \neq 0}} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right]$$

This satisfies a differential equation (prime denotes derivative with respect to z)

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

where $g_2(\tau) = 60G_4(\tau)$, $g_3(\tau) = 140G_6(\tau)$ with the Eisenstein series defined whenever $k \geq 3$ as

$$G_k(\tau) \;=\; \sum_{(m,n)\neq(0,0)} \frac{1}{(m\tau + n)^k}$$

With τ fixed, the map $z \to (\wp(z;\ \tau),\ \wp'(z;\ \tau))$ establishes an isomorphism of $\mathbf{C}/L_\tau$ with the elliptic curve whose equation is $y^2 = 4x^3 - Ax - B$ with $A = g_2(\tau)$, $B = g_3(\tau)$.

The Eisenstein series define modular forms. These will be discussed further in section 2.

1.6 Finite fields

Here the natural question to ask is for the number of rational points $\#E(\mathbf{F}_q)$. Recall that a finite field has a unique extension field of degree n, $\mathbf{F}_{q^n}$. We consider the generating series of the function $n \mapsto \#E(\mathbf{F}_{q^n})$. Actually it is preferable to consider the zeta function:

$$Z(E/\mathbf{F}_q, t) \;=\; \exp\left(\sum_{n=1}^{\infty} \#E(\mathbf{F}_{q^n}) t^n/n \right)$$

One reason is that this is a rational function of the variable t.

Theorem 1.2. *For an elliptic curve E over a finite field $\mathbf{F}_q$,*

$$Z(E/\mathbf{F}_q, t) \;=\; \frac{1 - a_q t + q t^2}{(1-t)(1-qt)}$$

The roots of the polynomial $1 - a_q t + qt^2$ have absolute value $q^{-1/2}$.

They were introduced by E. Artin in around 1920 in his Ph.D. thesis. The assertion about the roots in the above theorem is called the Riemann hypothesis, because it is an analogue of the conjecture made by Riemann about the classical zeta function. The zeta function for algebraic curves over finite fields were shown by F. K. Schmidt in the 1930's to be rational functions. Also in the 1930's H. Hasse proved the Riemann hypothesis for curves of genus 1, i.e., elliptic curves.

André Weil then proved the Riemann hypothesis for the zeta functions of arbitrary curves in 1940 (while in prison!). Later in the late 1940's he made a list of conjectures about the zeta functions of algebraic varieties of any dimension. These became known as the Weil Conjectues, and were the object of intense efforts in the next 25 years to prove them. The zeta function of an algebraic variety over a finite field is always a rational function, a theorem of first proved by Dwork using p-adic analysis, and then by Grothendieck using the theory of l-adic cohomology developed by him and his collaborators. The crowning triumph was Deligne's proof in 1973 of the analog of the Riemann hypothesis for the zeta function of an algebraic variety over a finite field.

For an elliptic curve, the zeta function is determined by knowledge of one number a_q, defined by $1 + q - a_q = \#E(\mathbf{F}_q)$. For example the elliptic curve E defined by $y^2 + y = x^3 - x^2$ has 10 rational points over $\mathbf{F}_{13}$, namely

$$\infty,\ (0,0),\ (0,12),\ (1,0),\ (1,12),\ (2,5),\ (2,7),\ (8,2),\ (8,10),\ (10,6)$$

Therefore

$$Z(E/\mathbf{F}_{13}, t) \;=\; \frac{1 - 4t + 13t^2}{(1-t)(1-13t)}$$

1.7 p - adic fields

Here we are referring to the finite extensions of the field of p - adic numbers $\mathbf{Q}_p$. Elliptic curves over these fields were first studied by Weil and his student Lutz in the 1930's. Since these fields are less generally familiar, we

will only mention a congruence property of the expansion coefficients of the invariant differential ω. To change notation slightly, define the elliptic curve by an equation $y^2 = x^3 + ax + b$, and the differential by $\omega = dx/2y$. Let $u = -x/y$. Then u is a local parameter on E in a neighborhood of O so we can expand quantities of interest in power series in u. One is the group law itself. If u_1 and u_2 are the parameters of two points P_1 and P_2 then the parameter of $P_1 + P_2$ is given by

$$\begin{aligned} F(u_1,\ u_2) &= u_1 + u_2 - 2au_1u_2 - 4a(u_1^3u_2^2 + u_1^2u_2^3) \\ &- 16b(u_1^3u_2^4 + u_1^4u_2^3) - 9b(u_1^5u_2^2 + u_1^2u_2^5) + \ldots \end{aligned}$$

This is called the *formal group* of E. The coefficients are polynomials in a, b with integer coefficients.

Another is the differential

$$\begin{aligned} \omega &= du(1 + 2au^4 + 3bu^6 + 6a^2u^8 + 20abu^{10} + \ldots) \\ &= \sum_{n=1}^{\infty} c(n)u^{n-1}du \end{aligned}$$

Formally integrating this series gives

$$f(u) = \sum_{n=1}^{\infty} c(n)u^n/n$$

This is called the logarithm of the formal group because

$$F(u,\ v) = f^{-1}(f(u) + f(v))$$

where $f^{-1}(u)$ is the inverse power series defined by $f^{-1}(f(u)) = u$. The following theorem was noted independently by a number of people (Atkin and Swinnerton - Dyer, Cartier, Honda)

Theorem 1.3. *Let E be an elliptic curve defined over the rational field $\mathbf{Q}$ and suppose that p is a prime of good reduction for E and that $1 - a_pt + pt^2$ is the numerator of its zeta function as an elliptic curve over $\mathbf{F}_p$. If the $c(n)$ are the expansion coefficients of the differential of the first kind as above, we have the congruences:*

1. *$c(p) \equiv a_p \ mod\ p$.*
2. *$c(np) \equiv c(n)c(p) \ mod\ p$ if GCD $(n, p) = 1$.*
3. *$c(np) - a_p\ c(n) + p\ c(n/p) \equiv 0 \ mod\ p^s$ for $n \equiv 0 \ mod\ p^{s-1}$, $s \geq 1$.*

See [2]. Actually one ought to assume that the equation for E is a so - called minimal one at p, but this will be so with a finite number of expectional p. Assume that $c(p) \neq 0 \mod p$; inductively it follows that $c(p^s) \neq 0 \mod p$ for all s. The Cartier - Honda congruences then show that the sequence of rational numbers

$$\frac{c(p^{s+1})}{c(p^s)}$$

is p - adically convergent to the reciprocal α of the root of $1 - a_p t + pt^2 = 0$ which is a p - adic unit (the other reciprocal root is p/α, which has p - adic value one).

There is a beautiful application of these ideas to congruence properties of special polynomials, discovered by Honda. In the Jacobi quartic family, consider the differential

$$\omega \;=\; \frac{dx}{\sqrt{1 - 2\kappa x^2 + x^4}} \;=\; \sum_{n=0}^{\infty} P_n(\kappa) x^{2n} dx$$

The polynomials $P_n(\kappa)$ are the Legendre polynomials that arise in the theory of spherical harmonics. The above congruences imply the following set of congruences discovered by Schur: Fix a prime p. If $n = a_0 + a_1 p + a_2 p^2 + \ldots + a_d p^d$ is the p - adic expansion of a given positive integer n, $0 \leq a_i < p$. Then

$$P_n(\kappa) \equiv P_{a_0}(\kappa) P_{a_1}(\kappa^p) \ldots P_{a_d}(\kappa^{p^d}) \mod p$$

See [13]

2 Modular forms

2.1 What they are.

Reference: [4], [7].
Consider the upper half - plane of complex numbers:

$$\mathbf{H} \;=\; \{\tau \in \mathbf{C} \mid \mathrm{Im}(\tau) > 0\}.$$

The group

$$\mathbf{SL}(2,\ \mathbf{R}) \;=\; \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{Mat}(2,\ \mathbf{R}) \mid ad - bc = 1 \right\}$$

operates on $\mathbf{H}$ by the rule

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau \;=\; \frac{a\tau + b}{c\tau + d}$$

This is the full group of holomorphic automorphisms of $\mathbf{H}$. The upper half plane also carries a non Euclidean geometry of constant negative curvature (the Lobatchevsian plane) whose geodesics are the circular arcs orthogonal to the real axis, and this group of transformations preserves this geometry, a fact first noted by Poincaré.

Let Γ be a subgroup of finite index in $\mathbf{SL}(2,\ \mathbf{Z})$. We get a Riemann surface by taking the quotient $Y(\Gamma) = \Gamma\backslash\mathbf{H}$. This is an open subset of a compact Riemann surface $X(\Gamma) = \Gamma\backslash\mathbf{H}^*$, and the complement $X(\Gamma) - Y(\Gamma)$ is a finite set of points called cusps. As is well-known, $X(\Gamma)$ is topologically a sphere with g handles attached. The number g is called the genus.

For instance if $\Gamma = \mathbf{SL}(2, \mathbf{Z})$, the genus is 0 and there is one cusp, so $X(\Gamma)$ is topologically a 2-sphere. Since there is one cusp, $Y(\Gamma) = \mathbf{C}$. These Riemann surfaces can be seen from the fundamental domain of the group and the gluing of the edges.

An interesting example of this is the group $\Gamma_0(11)$. We obtain in this way a Riemann surface of genus 1 with 2 cusps. This is the Riemann surface of an algebraic curve, in fact it is the elliptic curve $y^2 + y = x^3 - x^2$ we have considered before (at least up to isogeny). Pictures of the fundamental domains appear in the next pages.

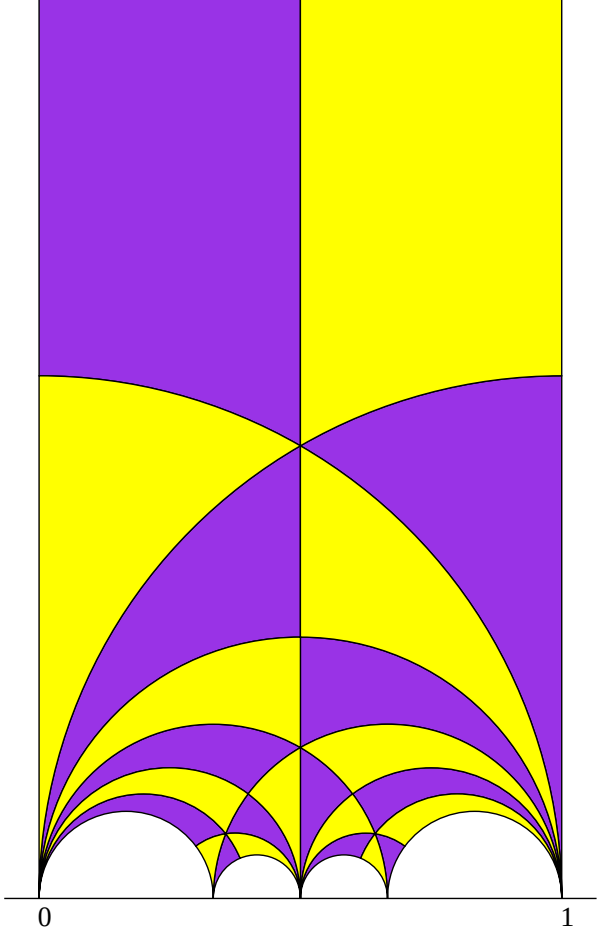

Figure 1: Fundamental domain for $\Gamma_0(11)$ showing translates of fundamental regions for $\mathrm{SL}_2(\mathbf{Z})$.

Definition 2.1. Let Γ be a subgroup of finite index in $\mathbf{SL}(2,\ \mathbf{Z})$. A modular form of weight k for Γ is a complex - valued function $f(\tau)$ defined in $\mathbf{H}$ such that

1. $f(\tau)$ is holomorphic.
2. $$f\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^k f(\tau) \quad \text{for all} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma.$$
3. $f(\tau)$ is holomorphic at all the cusps of Γ.

The third condition is a technical one; we can explain it in the important special case of the subgroup

$$\Gamma_0(N) \ = \ \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}(2,\ \mathbf{Z}) \mid c \equiv 0 \bmod N \right\}$$

Since the translation $\tau \to \tau + 1$ belongs to this group, the transformation property of modular forms shows that $f(\tau)$ is periodic, and therefore admits

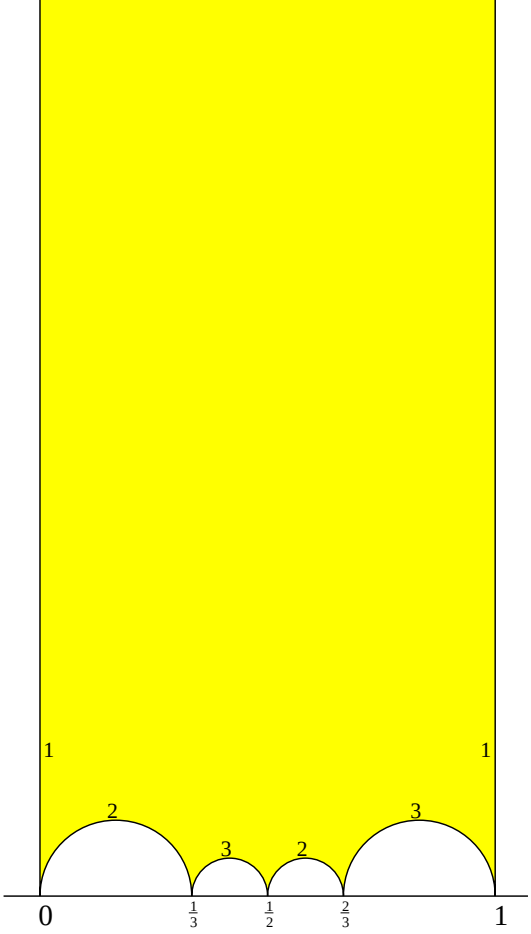

Figure 2: Fundamental domain for $\Gamma_0(11)$ showing the gluing data for the edges.

a Fourier expansion

$$f(\tau) \;=\; \sum a(n)q^n, \quad q = e^{2\pi i\tau}$$

We say that $f(\tau)$ is mermorphic at the cusp $i\infty$ if this expansion has only a finite number of negative exponents; that it is holomorphic if it has only nonnegative exponents; and that it is a cusp form if it is holomorphic and the constant term is zero: $a(0) = 0$. In general a subgroup such as $\Gamma_0(N)$ has a finite number of cusps, and there are corresponding q - expansions at each cusp. We impose these conditions at each cusp.

Examples of modular forms (for $\Gamma = \mathbf{SL}(2,\ \mathbf{Z})$) are the Eisenstein series previously defined. A suitable constant multiple of $G_k(\tau)$ has an expansion of the shape

$$1 + C_k \sum_{n=1}^{\infty} \sigma_{k-1}(n)q^n, \quad \sigma_s(n) \;=\; \sum_{0<d|n} d^s$$

where the constant $C_k \in \mathbf{Q}$ is related to the Bernoulli numbers. These have weight k. In general, the expansion coefficients of modular forms are

arithmetical functions with interesting properties. In this example we have for instance

$$\sigma_s(mn) \;=\; \sigma_s(m)\sigma_s(n) \;\text{ whenever }\; \mathrm{GCD}(m,n)=1$$

An example of a cusp form (weight 12) is Δ defined by

$$\Delta(\tau) \;=\; g_2(\tau)^3 - 27g_3(\tau)^2$$

This has the expansion

$$(2\pi)^{-12}\Delta(\tau) \;=\; \eta(\tau)^{24} \;=\; q\prod_{n=1}^{\infty}(1-q^n)^{24} \;=\; \sum_{n=1}^{\infty}\tau(n)q^n$$

for an arithmetical function $n \to \tau(n)$ introduced and studied by Ramanujan. This $\tau(n)$ is not to be confused with the τ in the upper half plane. He conjectured the following properties:

1. $\tau(mn) \;=\; \tau(m)\tau(n)$ whenever GCD $(m,n)=1$.
2. $\tau(p^s)\tau(p) = \tau(p^{s+1}) + p^{11}\tau(p^{s-1})$ for a prime p, $s \geq 1$.
3. $\tau(m) \;=\; \mathrm{O}(m^{11/2})$

The first two of these were proved by Mordell, but it was only after the Hecke operators were introduced that these formulas were really understood. Note that the first two conditions have as consequence that Ramanujan's $\tau(n)$ is entirely determined by a function on the prime numbers $p \to \tau(p)$. Indeed this may be formally expressed as an equality of Dirichlet series

$$L(\Delta,\; s) := \sum_{n=1}^{\infty}\tau(n)/n^s \;=\; \prod_{p}\left(1-\tau(p)p^s+p^{11-2s}\right)^{-1}$$

This is known to possess an analytic continuation to an entire function of the complex variable s, which has a functional equation: the function $(2\pi)^{-s}\Gamma(s)L(\Delta,\; s)$ is invariant under the substitution $s \to 12-s$. These properties are analogous to those of the Riemann zeta function

$$\zeta(s) := \sum_{n=1}^{\infty}1/n^s \;=\; \prod_{p}\left(1-p^{-s}\right)^{-1}$$

The analytic properties of the Dirichlet series associated to modular forms lie at the heart of modern researches in the arithmetic of automorphic forms. For any cusp form $f(\tau)$ for $\Gamma_0(N)$ one can introduce a Dirichlet series

$$L(f,\ s)\ =\ \sum_{n=1}^{\infty} a(n)/n^s$$

where the coefficients are the q - expansion coefficients of $f(\tau)$. It possesses an "Euler product" expansion over all the primes as in the example of Δ if and only if it is an eigenfunction for all the Hecke operators.

As for the third condition conjectured by Ramanujan, it was proved by Deligne when he established the Riemann hypothesis for the congruence zeta functions of algebraic varieties alluded to above. More precisely, it had been previously established by several mathematicians, notably by Ihara, Kuga and Deligne, that Ramanujan's third conjecture would be a corollary of the Weil conjectures.

An example of a meromorphic modular form of weight 0 is J defined as

$$J(\tau)\ =\ 1728\ g_2(\tau)^3/\Delta(\tau)$$

whose expansion has integer coefficients, and begins

$$q^{-1}\ +\ 744\ +\ 196884q\ +21493760q^2\ +\ \ldots$$

This function has the important property that the elliptic curves defined by lattices L_{τ_1} and L_{τ_2} are isomorphic if and only if $J(\tau_1) = J(\tau_2)$.

2.2 Wiles' theorem

As we have seen, elliptic curves and modular forms are related to each other. This fact was already clear in the 19 th century - the moduli of elliptic curves are expressible in terms of modular forms of the parameter τ in the upper half plane. However, in the 1950's a new sort of relation between elliptic curves and modular forms was perceived, first by Taniyama, then more precisely by Shimura and Weil.

Let E be an elliptic curve defined over $\mathbf{Q}$, say by an equation $y^2\ = 4x^3 - Ax - B$ with rational integers A, B. For every prime p not dividing the discriminant $\Delta = A^3 - 27B^2$, we get an elliptic curve over the finite field $\mathbf{F}_p$ with this equation. We therefore have its zeta function, the numerator of which is of the shape $1 - a_p t + pt^2$, with a_p defined by counting the number of solutions to the congruence $y^2\ \equiv\ 4x^3 - Ax - B \bmod p$,

$$1 - a_p + p = \#E(\mathbf{F}_p)$$

Note that $\#E(\mathbf{F}_p)$ is actually one more than the number of solutions to the congruence, since E has one point at infinity in the projective plane. Following Hasse, we put these polynomials together by replacing t by p^{-s} for a complex variable s and forming the product

$$L(E,s) \;=\; \prod_p \left(1 - a_p p^{-s} + p^{1-2s}\right)^{-1}$$

One ought to put in factors corresponding to the finitely many primes for which our curve E becomes singular, namely the prime divisors of the discriminant. This can be done, but it is technical to explain. Assume that it has been done. Then Wiles' big theorem, conjectured by Taniyama, Shimura and Weil, is

Theorem 2.1. *For every elliptic curve E defined over the field of rationals $\mathbf{Q}$ there exists $f(\tau)$, a cusp form of weight 2 for a subgroup $\Gamma_0(N)$, such that*

$$L(f,\ s) \;=\; L(E,\ s)$$

See [12], [10].
Wiles and Taylor only proved this for so-called *semistable* elliptic curves, which was sufficient to prove Fermat's last theorem. The general case was done in [1]. The integer N is computed from the elliptic curve as the *conductor* of E. This is an integer related to the discriminant, but whose definition is too technical to explain here.

In down - to - earth terms Wiles' theorem says the following: Take an elliptic curve E say defined by an equation of the form $g(x,\ y) = 0$ with for a polynomial with integer coefficients g, and for any prime p not dividing its discriminant, count up the number $\#E(\mathbf{F}_p)$ of solutions to the congruence $g(x,\ y) \equiv 0 \bmod p$ including the point(s) at infinity. Write it in the form $\#E(\mathbf{F}_p) \;=\; 1 + p - a_p(E)$. *Then the integer* $a_p(E)$ is the p th *Fourier coefficient of a cusp form of weight 2.*

Example. The curve $y^2 + y = x^3 - x^2$ discussed before. This has conductor 11. The corresponding modular form is

$$\begin{aligned}
\eta(\tau)^2\eta(11\tau)^2 \quad &= \quad q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2 \\
&= \quad q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 \\
&- \quad 2q^9 - 2q^{10} + q^{11} - 2q^{12} + 4q^{13} - q^{15} + \ldots
\end{aligned}$$

We found before that there were 10 points on this curve over the field with 13 elements. This is predicted by the above expansion because the 13 th coefficient is 4: $10 = 1 + 13 - 4$. This works for every prime except 11.

Example. The curve $y^2 + xy - y = x^3$. This has conductor 14. The corresponding modular form is

$$\begin{aligned}\eta(\tau)\eta(2\tau)\eta(7\tau)\eta(14\tau) &= q\prod_{n=1}^{\infty}(1-q^n)(1-q^{2n})(1-q^{7n})(1-q^{14n}) \\ &= q - q^2 - 2q^3 + q^4 + 2q^6 + q^7 - q^8 \\ &+ q^9 - 2q^{12} - 4q^{13} - q^{14} + q^{16} + \dots\end{aligned}$$

We find that there are 18 points on this curve over the field with 13 elements:

$$\begin{array}{cccccccc}\infty, & (0,0), & (0,1), & (1,1), & (1,12), & (5,3), & (5,6), & (7,9), & (7,11) \\ (8,2), & (8,4), & (9,7), & (9,11), & (10,6), & (10,11), & (11,6), & (11,10), & (12,1)\end{array}$$

This is predicted by the above expansion because the 13 th coefficient is -4: $18 = 1 + 13 - (-4)$. This works for all primes except 2 and 7.
Example. The curve $x^3+y^3 = 1$. This has conductor 27. The corresponding modular form is

$$\begin{aligned}\eta(3\tau)^2\eta(9\tau)^2 &= q\prod_{n=1}^{\infty}(1-q^{3n})^2(1-q^{9n})^2 \\ &= q - 2q^4 - q^7 + 5q^{13} + 4q^{16} - 7q^{19} - 5q^{25} \\ &+ 2q^{28} - 4q^{31} + 11q^{37} + 8q^{43} - 6q^{49} + \dots\end{aligned}$$

This has 3 points on the line at infinity for $p \equiv 1 \bmod 3$, and one point on the line at infinity if $p \equiv 2 \bmod 3$. One has that $\#E(\mathbf{F}_p) = p + 1$ if $p \equiv 2 \bmod 3$, and $\#E(\mathbf{F}_p) = p + 1 - a$ for $p \equiv 1 \bmod 3$, where a is determined by the following recipe due to Gauss: for any prime congruent to 1 mod 3 we can write $4p = a^2 + 27b^2$ in integers in a unique way up to the signs of a and b. We choose a so as to satisfy the congruence $a \equiv 2 \bmod 3$, and this fixes the sign. Of course, this a is also the p th coefficient of the above series (note that the p th coefficient of the series is 0 if $p \equiv 2 \bmod 3$). This alternate method of writing the number of solutions of the congruence is a reflection of the fact that the elliptic curve $x^3 + y^3 = 1$ has "complex multiplications". For instance $4 \cdot 13 = (\pm 5)^2 + 27(\pm 1)^2$, so we choose $a = 5$ to satisfy the congruence mod 3. Then we are predicted to have $p + 1 - a = 13 + 1 - 5 = 9$ points on this curve over $\mathbf{F}_{13}$. In addition to the 3 points at infinity, we have

$$(0,1),\ (0,3),\ (0,9),\ (1,0),\ (3,0),\ (9,0)$$

This works for all primes except 3.

Example. The curve $y^2 = 4x^3 + 68$. This has conductor $(2 \cdot 3 \cdot 17)^2 = 10404$. The corresponding modular form is

$$\begin{aligned} f(\tau) &= q - 5q^7 - 7q^{13} - 7q^{19} - 5q^{25} - 11q^{31} - 11q^{37} \\ &- 13x^{43} + 18x^{49} + 13x^{61} + 5x^{67} + 10x^{73} + 4x^{79} + \ldots \end{aligned}$$

We find that there are 13 points on this curve over the field with 7 elements:

$$\begin{array}{cccccc} \infty, & (1,3), & (1,4), & (2,3), & (2,4), & (3,1), & (3,6) \\ (4,3), & (4,4), & (5,1), & (5,6), & (6,1), & (6,6) \end{array}$$

This agrees with the coefficient of q^7 in f, namely, $13 = 7 + 1 - (-5)$.

The expansion coefficients of these modular forms are arithmetical functions that satisfy identities similar to those of the Ramanujan τ function:

1. $a(mn) = a(m)a(n)$ whenever GCD $(m, n) = 1$.
2. $a(p^s)a(p) = a(p^{s+1}) + p\ a(p^{s-1})$ for a prime p, $s \geq 1$.
3. $a(m) = \mathrm{O}(m^{1/2})$

These hold only for coefficients $a(m)$ with m prime to N.

References

[1] Breuil, C.; Conrad, B.; Diamond, F.; Taylor, R. *On the modularity of elliptic curves over* **Q***; wild 3-adic exercises*, J. Amer. Math. Soc. 14 (2001), 843-939.

[2] Cartier, P., *Groupes formels, fonctions automorphes, et fonctions zeta des courbes elliptiques*, Actes, 1970 Congrés Intern. Math. Tome 2 (1971) 291 - 299.

[3] Cassels, J. W. S., "Lectures on Elliptic Curves", London Math. Soc. Student Texts **24** Cambridge U. Press, 1991.

[4] Diamond, F. and Shurman J. "A first course in modular forms", GTM, 228, Springer-Verlag, 2005.

[5] Knapp, A. W., "Elliptic Curves", Math. Notes **40** Princeton U. Press, 1992.

[6] Milne, J., "Elliptic curves", BookSurge Publishers, Charleston, S.C., 2006.

[7] Miyake, T., "Modular Forms", Springer - Verlag, 1989.

[8] Silverman, J. H., (1)" The Arithmetic of Elliptic Curves", Grad. Texts in Math. **106** Springer - Verlag, 1986; (2) " Advanced Topics in the Arithmetic of Elliptic Curves", Grad. Texts in Math. **151** Springer - Verlag, 1994.

[9] Silverman, J. H. and Tate, J., "Rational Points on Elliptic Curves", Undergraduate Texts, Springer - Verlag, 1992.

[10] Taylor, R. and Wiles, A., *Ring theoretic properties of certain Hecke algebras*, Ann. of Math. **141** (1995) 553 - 572.

[11] Weil, A., "Number Theory. An approach through history. From Hammurapi to Legendre", Birkhäuser, Boston - Basel - Stuttgart, 1984.

[12] Wiles, A., *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. **141** (1995) 443 - 551.

[13] Yui, N., *Jacobi quartics, Legendre polynomials, and formal groups*, Lecture Notes in Math **1326**, Springer, 1988, 182 - 215.