Elliptic Functions and Modular Forms

François Morain
École Polytechnique

March, 7, 1994

[summary by Daniel Augot]

Abstract

Up to now, there is no good algorithm for computing logarithms in a general finite abelian group. Elliptic curves over finite fields present examples of such groups, and are good candidates for constructing cryptosystems based on exponentiation. To do so, one needs a generator, and to be able to find one, the order of the elliptic curves must be known. It can be computed with machines, and prime numbers up to 250 digits can be dealt with. This first talk introduces the material about elliptic curves, modular forms, ... which is necessary for describing *modular equations*, while the second talk describes algorithms for finding the order of an elliptic curve, specially the "Schoof-Atkin-Elkies" algorithm. Recent work by Couveignes gives an improvement of the method.

1. Elliptic functions

First a whole bunch of definitions, theorems and examples are presented, which are a bit classical.

1.1. Lattices, Eisenstein's series. At the beginning of time, there were lattices:

DEFINITION 1. A *lattice* $\mathbb{L}$ is $\mathbb{L} = \mathbb{Z}\omega_2 + \mathbb{Z}\omega_1$, where $\tau = \omega_1/\omega_2 \in \mathcal{H}$ the upper half-plane. A *cell* is $\{\lambda\omega_1 + \mu\omega_2 + z,\ (\lambda, \omega) \in (0,1)^2\}$, for $z \in \mathbb{C}$.

The following definitions are related to a given lattice.

DEFINITION 2. A meromorphic function f on $\mathbb{C}$ is an *elliptic function* if and only if f is doubly periodic: $\forall z \in \mathbb{C},\ f(z+\omega_1) = f(z+\omega_2) = f(z)$.

PROPOSITION 1. *Let f be an elliptic function. The number of poles and the number of zeroes in a cell is finite. The sums of the residues at poles is 0. An elliptic function with no poles is a constant.*

DEFINITION 3 (WEIERSTRASS'S $\wp$ FUNCTION). The *Weierstrass's $\wp$ function* associated to the lattice $\mathbb{L}$ is

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \mathbb{L},\, \omega \neq 0} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

PROPOSITION 2. *Weierstrass's $\wp$ function is differentiable, and*

$$\wp' = -2 \sum_{\omega \in \mathbb{L}} \frac{1}{(z-\omega)^3}.$$

The functions $\wp$ and $\wp'$ are periodic on $\mathbb{L}$, and the field of elliptic functions is $\mathbb{C}(\wp, \wp'')$.

Starting from:

$$\frac{1}{(z-\omega)^2} = \frac{1}{\omega^2\left(1-\frac{z}{\omega}\right)^2} = \frac{1}{\omega^2} + \frac{2z}{\omega^3} + \cdots + \frac{kz^{k-1}}{\omega^{k+1}} + \cdots,$$

the expansion of $\wp$ near the origin is

$$\wp = \frac{1}{z^2} + 2zG_3(\mathbb{L}) + 3z^2G_4(\mathbb{L}) + \cdots + kz^{k-1}G_{k+1}(\mathbb{L}) + \cdots$$

where

$$G_k(\mathbb{L}) = \sum_{\omega\in\mathbb{L},\omega\neq 0} \frac{1}{\omega^2}.$$

We also denote $G_k(\tau)$ the function $G_k(1,\tau)$. The functions $g_2(z)$ and $g_3(z)$ are $g_2(z) = 60G_4(z)$, $g_3(z) = 140G_6(z)$. The *Eisenstein's series* are $E_k(\tau) = G_k(\tau)/(2\zeta(k))$, $k \geq 2$

THEOREM 1. *Let τ be given, and $g_2 = g_2(\tau)$, $g_3 = g_3(\tau)$. Let C be the curve defined by the equation*

$$y^2 = 4x^3 - g_2x - g_3.$$

Then:

(1) *the equation $4x^3 - g_2x^2 - g_3 = 0$ has three distinct roots,*
(2) *the curve C is* parameterized *par $\wp, \wp'$: for each point (x,y) of C, there exists $z \in \mathbb{C}$ such that $(x,y) = (\wp(z), \wp'(z))$.*

Conversely, if C is a curve given by the equation $y^2 = 4x^3 - a_2x - a_3$, such that $4x^3 - a_2x - a_3$ has three distinct roots in $\mathbb{C}$, then there is a lattice $\mathbb{L}$ such that $a_2 = g_2(\mathbb{L})$ and $a_3 = g_3(\mathbb{L})$. The function $\wp_{\mathbb{L}}$ and its derivative yield a parameterisation of C.

2. Modular Functions and modular forms

2.1. Definitions.

DEFINITION 4. The *Poincaré half-plane* is defined as $\mathcal{H} = \{z \in \mathbb{C}, \mathcal{I}(z) > 0\}$, $\mathcal{I}(z)$ standing for the imaginary part of $z \in \mathbb{C}$. The *modular group* Γ is the set of matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad \text{with} \quad (a,b,c,d) \in \mathbb{Z}^4,\ ad - bc = 1.$$

The matrices $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ are the classical generators of Γ. An action of Γ on $\mathcal{H}$ is defined by

$$\forall M \in \Gamma, \forall \tau \in \mathcal{H}, M\tau = \frac{a\tau + b}{c\tau + d}.$$

At last $\mathcal{H}^\star = \mathcal{H} \cup \mathbb{Q} \cup i\infty$ is a compactification of $\mathcal{H}$.

DEFINITION 5. $f : \mathcal{H}^\star \to \hat{\mathbb{C}}$ is a *modular function of weight* k if and only if:

(1) f is meromorphic on $\mathcal{H}$,
(2) $\forall M \in \Gamma, \forall \tau \in \mathcal{H}^\star, f(M\tau) = (c\tau + d)^k f(\tau)$.

If $f(i\infty) \in \mathbb{C}$, then f is a *modular form*, and if $f(i\infty) = 0$, f is a *cusp form.*

EXAMPLE. The Eisenstein's series $E_k(\tau)$ is a modular form of weight k, $k > 2$.

PROPOSITION 3. *There exists no modular form of odd weight k. If f is of weight k and g of weight k', then fg is of weight $k + k'$, f/g of weight $k - k'$.*

EXAMPLE.

- $\Delta(\tau) = (2\pi)^{12}\left(E_4^3(\tau) - E_6(\tau)^2\right)/1728$ is a cusp form of weight 12 ;
- the modular invariant $j(\tau) = 1728 g_2^3(\tau)/\Delta(\tau)$ is a function of weight 0 ;
- $(2\pi)^{-12}\Delta(q)$ can be proven to be equal to $\eta(q)^{24}$, where $\eta(q) = q^{1/24}\prod_{n=1}^{\infty}(1-q^n)$ is the η function.

THEOREM 2. *Let f be a meromorphic function on $\mathcal{H}$. The following statements are equivalent:*

(1) *f is a modular function of weight 0 ;*
(2) *f is the quotient of two modular forms of same weight ;*
(3) *$f \in \mathbb{C}(j)$.*

Let $\mathcal{M}_k$ be the vector space of modular functions of weight k. If $k = 2$ or $k < 0$ then $M_k = \{0\}$, if $k = 4, 6, 8, 10$ then $\mathcal{M}_k$ is of dimension 1 generated by E_k. $\mathcal{M}_1$ is generated by 1.

As a consequence, it is easy to show that $E_8 = E_4^2$, $E_{10} = E_4 E_6$. The Eisenstein series E_2 is not a form, since

$$E_2(-1/\tau) = \tau^2 E_2(\tau) + \frac{12\tau}{2i\pi}.$$

2.2. Modular forms for subgroups. Let Γ_1 be a subgroup of Γ of finite index.

EXAMPLE. Let $\Gamma_0(\ell)$ be the subgroup of matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, with $c \equiv 0 \bmod \ell$. The index $\mu_0(\ell)$ of $\Gamma_0(\ell)$ is $\mu_0(\ell) = \ell\prod_{p|\ell}(1+1/p)$.

DEFINITION 6. $\mathcal{F}_1$ is a *fundamental set* for Γ_1 if and only if any point of $\mathcal{H}^\star$ is equivalent (modulo Γ_1) to a unique point in $\mathcal{F}_1$. $\mathcal{F}_1$ is a *fundamental region* if the conditions

$$\tau \in \mathcal{F}_1, \quad \exists M \in \Gamma_1, M \neq 1, M\tau \in \mathcal{F}_1$$

implie that τ belongs to the boundary of $\mathcal{F}_1$.

THEOREM 3. *Let Γ_1 be a finite subgroup of finite index μ, and $\{S_v\}_{1\le v\le\mu}$ be a set of coset representatives of Γ_1, i.e.*

$$\Gamma/\Gamma_1 = \{\bar{S_v}\}_{1\le v\le\mu}.$$

Then

$$\mathcal{F}_1 = \bigcup_{v=1}^{\mu} S_v(\mathcal{F})$$

is a fundamental region for Γ_1.

2.3. Modular equations.

DEFINITION 7. A function f on $\mathcal{H}^\star$ is a *modular function* for Γ_1 if and only if

(1) f is meromorphic on $\mathcal{H}$,
(2) $\forall M \in \Gamma_1, \forall\tau \in \mathcal{H}^\star, f(M\tau) = f(\tau)$.

It works naturally: if f is a function for a subgroup Γ_1, then $f \circ M$, denoted $f\,|_M$, is a function for the conjugate of Γ_1 by M. A function for a subgroup is a function for its subgroups.

THEOREM 4. *Let f be a function for Γ_1. Set*

$$G(X) = \prod_{v=1}^{\mu} (X - f\,|_{S_v}).$$

The polynomial $G(X)$ can be written

$$G(X) = \sum_{v=0}^{\mu} R_v(j) X^v,$$

where $R_v(j) \in \mathbb{C}(j)$. Then $G(f(q)) = 0$. Such an equation is called a modular equation *for Γ_1. If $f = \sum a_n q^n$ has integer coefficients coefficients, then $G(X, j)$ has integer coefficients.*

EXAMPLE. (Canonical modular equation for $\Gamma_0(\ell)$)
Let $s = 12/\gcd(12, \ell - 1)$, and $v = s(\ell - 1)/12$. The function

$$f(\tau) = \ell^s \left(\frac{\eta(\ell\tau)}{\eta(\tau)}\right)^{2s} = q^v + \sum_{n=v+1}^{\infty} a_n q^n,$$

is a function for $\Gamma_0(\ell)$. The modular equation for f is

$$\Phi_\ell^c(X, j) = (X - f(\tau)) \prod_{k=0}^{\ell-1} (X - f(-1/(1 + k\tau))). \tag{1}$$

Let w_ℓ be the operation associated to

$$\begin{pmatrix} 0 & -1 \\ \ell & 0 \end{pmatrix}.$$

The application w_ℓ is an involution (the *Atkin-Lehmer* involution), and if f is a function for $\Gamma_0(\ell)$, so is $f \circ w_\ell$. Using the Atkin-Lehmer involution, the equation (1) is transformed into

$$P(Y, j) = (Y - \ell^s/f(\tau)) \prod_{k=0}^{\ell-1} (Y - f((\tau + k)/\ell)) = Y^{\ell+1} + \sum_{r=0}^{\ell} C_r(j) Y^r,$$

with $\deg(C_r(j)) \leq v - \frac{rv}{\ell}$. The power-sum symmetric functions

$$S_r = (\ell^s/f(\tau))^r + \sum_{k=0}^{\ell-1} f((\tau + k)/\ell)^r$$

can be computed, and thus the coefficients $C_r(j)$, by Newton's identities.

Bibliography

[1] Atkin (A. O. L.). – The number of points on an elliptic curve modulo a prime. – Preprint, 1988.

[2] Schoeneberg (B.). – *Elliptic modular functions.* – Springer-Verlag, 1974, *Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen*, vol. 203.

[3] Serre (J.-P.). – *Cours d'arithmétique.* – Presses Universitaires de France, 1970.