Elliptic Curves and Complex Multiplication

Michel Waldschmidt

November 11, 1997

Saint-Etienne, May 1982
Notes by A. Faisant, R. Lardon, G. Philibert

1 Introduction

A calculator can give you the decimal expansion

$$e^{\pi\sqrt{163}} = 262\,537\,412\,640\,768\,743.9999999999992\ldots$$

In spite of its appearance this number is not an integer since it is transcendent by the theorem of Gel'fond-Schneider:

$$e^{\pi\sqrt{163}} = (e^{i\pi})^{-i\sqrt{163}} \text{ with } \begin{cases} e^{i\pi} \text{ algebraic, and} \\ -i\sqrt{163} \text{ irrational and algebraic.} \end{cases}$$

In order to explain the fact that $e^{\pi\sqrt{163}}$ is very close to an integer one starts with the observation that $\mathbb{Q}(\sqrt{-163})$ has class number 1; this implies that the modular function $j(\tau)$ is an integer for $\tau = \frac{1}{2}(1+i\sqrt{163})$. Expressing $j(\tau)$ by a Laurent series

$$j(\tau) = \frac{1}{q} + 744 + 196\,884q + 21\,493\,760q^2 + \ldots,$$

where $q = e^{2i\pi\tau} = -e^{-\pi\sqrt{163}}$. This gives

$$|j(\tau) - \frac{1}{q} - 744| \;=\; |-e^{\pi\sqrt{163}} - j(\tau) + 744| \;=\; 196\,884q + 21\,493\,760q^2 + \ldots,$$

and since $|q| < \frac{1}{2}10^{-17}$, one deduces that the distance of $-e^{\pi\sqrt{163}}$ from the integer $j(\tau) - 744$ is smaller than 10^{-12}.

There is an analogous situation for $\mathbb{Q}(\sqrt{-67})$: with $\tau = \frac{1}{2}(1+i\sqrt{67})$, we have $j(\tau) = -(5280)^3 = 147\,197\,952\,000$, and $e^{\pi\sqrt{67}}$ is very close to $147\,197\,952\,000$.

In general, we have $j(\tau) = \frac{1728g_2^3}{g_2^3-27g_3^2}$, where $g_2 = 60G_2$, $g_3 = 140G_3$, and where $G_k(z)$ is the Eisenstein series

$$G_k(z) = z^{2k} \sum_{(m,n)\in\mathbb{Z}^2\setminus\{(0,0)\}} (m+nz)^{-2k},$$

amd where the coefficient 1728 was inroduced so that the residue of $j(z)$ at infinity equal 1.

1728 has the following bizarre property: $1729 = 12^3 + 1^3 = 10^3 + 9^3$, and 1729 is the smallest integer which can be written in two different ways as the sum of two cubes.

It is known (Siegel 1929) that the equation $x^3 + 1 = 489y^2$ only has a finite number of integral solutions; one of them is quite large: $x = 53\,360$ and $y = 557\,403$, the reason for this being that $489 = 3 \cdot 163$ and that $\mathbb{Q}(\sqrt{-163}\,)$ has class number 1 ([1]).

Similarly, if $h(-p) = 1$, then the equation $x^3 - py^2 = -1728$ has an integral solution obtained by letting x be the nearest integer to $e^{\pi\sqrt{p}/3}$; this has to do with the fact that $j(\tau)$ is a perfect cube and that $\frac{1}{p}(1728 - j(\tau))$ is a square ([1]). The equation $x^3 - py^2 = -1728$ can be transformed (for $p = 163$) into $X^3 + 1 = 489Y^2$ by putting $x = 12X$ and $y = 72Y$.

Finally, the polynomial $x^2 - x + 41$ discovered by Euler takes only prime values for $x = 0, 1, \ldots, 40$: this result is also connected to the fact that $\mathbb{Q}(\sqrt{-163}\,)$ has class number 1: the discriminant of $x^2 - x + 41$ equals -163.

These results show the intimate connections which connect the class numbers of imaginary quadratic number fields and the modular invariant j. Weber has shown that the abelian closure of $\mathbb{Q}$ (i.e. the maximal abelian extension of $\mathbb{Q}$) can be obtained by adjoining the numbers $e^2\pi ir$ to $\mathbb{Q}$, where $r \in \mathbb{Q}$. In other words: by adjoining special values of the exponential function. Kronecker's 'Jugendtraum' from 1880 consisted in the hope that the abelian closure of a number field K can likewise be obtained by adjoining to K values of special functions. This question was taken up by Hilbert in his 12th problem, which consists of two parts: computation of the maximal unramified abelian extension, then of the abelian closure. If, for example, $K = \mathbb{Q}(\tau)$ is imaginary quadratic, its maximal unramified abelian extension is its Hilbert class field $L = K(j(\tau))$, and its degree over K is just the class number of K. The solution of Hilbert's 12th problem makes use of algebraic curves and special functions: if e.g. K is imaginary quadratic, the curve is an elliptic curve and the function is the modular function j. More generally, if K is a CM-field, i.e. a totally complex quadratic extension of a totally real number field, then Shimura has shown that the maximal unramified abelian extension of K can be obtained via varieties with complex multiplication and special values of automorphic functions ([2]).

2 Endomorphisms of elliptic curves

An elliptic curve can be defined in five different ways:

1. a connected compact Lie group of dimension 1,
2. a complex torus $\mathbb{C}/L$, where L is a lattice in $\mathbb{C}$,
3. a Riemann surface of genus 1,
4. a non-singular cubic in $\mathbb{P}_2(\mathbb{C})$,

5. an algebraic group of dimension 1, with underlying projective algebraic variety.

2.1 Homomorphisms

If M and L are two lattices one is interested in the analytic homomorphisms $\mathbb{C}/M \longrightarrow \mathbb{C}/L$. To this end, it is convenient to observe that the canonical surjection $s_L : \mathbb{C} \longrightarrow \mathbb{C}/L$ is the universal covering of $\mathbb{C}/L$ in the sense that, for each analytic homomorphism $\phi : \mathbb{C} \longrightarrow \mathbb{C}/L$, there exists a unique linear map $\lambda : \mathbb{C} \longrightarrow \mathbb{C}$ which makes the following diagram commutative:

$$\begin{tikzcd} \mathbb{C} \arrow[r, "\lambda"] \arrow[dr, "\phi"'] & \mathbb{C} \arrow[d, "s_L"] \\ & \mathbb{C}/L \end{tikzcd}$$

In fact, $s_L(0) = 0$ and s_L is continuous in 0, hence locally injective in a vicinity U of 0. Thus $\sigma = s_{L|U} : U \longrightarrow V$ is a bijection, and $f := \sigma^{-1} \circ \phi$ is analytic and respects addition in a vicinity W of 0: for $x, y, x + y \in W$. Taking the derivative with respect to y this gives $f'(x+y) = f'(y)$, and letting $y = 0$ yields $f'(x) = f'(0) = \lambda$, hence $f(x) = \lambda x$ (since $f(0) = 0$). Now $s_L(\lambda x) = \phi(x)$ in a vicinity of 0, hence everywhere, since the function $s_L(\lambda x) - \phi(x)$ is analytic and vanishes in a vicinity of 0.

If now $f : \mathbb{C}/L \longrightarrow \mathbb{C}/M$ is an analytic homomorphism, then $\phi = f \circ s_L : \mathbb{C} \longrightarrow \mathbb{C}/M$ factors through a $\lambda \in \mathbb{C}$ and one finds $s_M \circ \lambda = f \circ s_L$.

$$\begin{tikzcd} \mathbb{C} \arrow[r, "\lambda"] \arrow[d, "s_L"'] \arrow[dr, "\phi"'] & \mathbb{C} \arrow[d, "s_M"] \\ \mathbb{C}/L \arrow[r, "f"'] & \mathbb{C}/M \end{tikzcd}$$

This implies $\lambda L \subseteq M$.

If $f \neq 0$, then f is surjective: for $x + M \in \mathbb{C}/M$ one has $f(x\lambda^{-1} = L) = x + M$; moreover, $G = \operatorname{im} f$ is a compact subgroup of $\mathbb{C}/M$ (since f is a continuous homomorphism), hence G is closed. Now f is open (since it is analytic and not constant), hence G is also open in $\mathbb{C}/M$, which implies that $G = \mathbb{C}/M$ by connectivity. Next $\ker f$ is finite (since it is discrete inside a compactum – it is formed by isolated points): we say that f is an *isogeny* and write $\deg f = \# \ker f$.

Conversely, if $\lambda L \subseteq M$ for some $\lambda \in \mathbb{C}^\times$, then $f(x + L) = \lambda x + M$ defines an isogeny $\mathbb{C}/L \longrightarrow \mathbb{C}/M$. Since in this case there also exists a $\mu \in \mathbb{C}^\times$ such that $\mu M \subseteq L$ (this is a property of lattices), we see that there also exists an isogeny $\mathbb{C}/M \longrightarrow \mathbb{C}/L$. We say that $\mathbb{C}/L$ and $\mathbb{C}/M$ are *isogenous*.

2.2 Isomorphisms

Let $f : \mathbb{C}/L \longrightarrow \mathbb{C}/M$ be an analytic isomorphism. By what we have seen above f factors through a linear map $\mathbb{C} \longrightarrow \mathbb{C} : z \longmapsto \lambda z$ via the canoncical surjections $\mathbb{C} \longrightarrow \mathbb{C}/L$ and $\mathbb{C} \longrightarrow \mathbb{C}/M$ with $\lambda \in \mathbb{C}$ and $\lambda L \subseteq M$. The inverse isomorphism $f^{-1} : \mathbb{C}/M \longrightarrow \mathbb{C}/L$ factors through $z \longmapsto \frac{1}{\lambda} z$, hence $\lambda^{-1} M \subseteq L$. We deduce that $\lambda L = M$.

We will show that the modular invariant actually characterizes the isomorphism classes of elliptic curves:

$$\begin{aligned}
\wp_L(z) &= z^{-2} + \sum_{\omega \in L^\times} \Big(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \Big), \\
\wp_L'(z)^2 &= 4\wp_L(z)^3 - g_2(L)\wp_L(z) - g_3(L), \\
g_2(L) &= 60 \sum_{\omega \in L^\times} \omega^{-4} \quad \text{and} \quad g_3(L) \;=\; 140 \sum_{\omega \in L^\times} \omega^{-6}.
\end{aligned}$$

If $\lambda L = M$, then

$$\begin{cases} \wp_M(\lambda z) = \wp_{\lambda L}(\lambda z) = \lambda^{-2} \wp_L(z), \\ g_2(M) = \lambda^{-4} g_2(L), \\ g_3(M) = \lambda^{-6} g_3(L). \end{cases}$$

We define

- the discriminant: $\Delta(L) = g_2^3(L) - 27 g_3^2(L)$,
- the modular invariant: $j(L) = 1728 g_2^3(L)/\Delta(L)$.

Taking the preceding properties into account, we find

$$j(M) = j(L).$$

The lattice $L = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ can be written in the form $L = \omega_1(\mathbb{Z} + \tau\mathbb{Z})$, where $\tau = \omega_2/\omega_1$ and $\operatorname{Im}\tau > 0$. Thus $j(L) = j(\mathbb{Z} + \tau\mathbb{Z}) =: j(\tau)$; this defines a map $j : \mathbb{H} \longrightarrow \mathbb{C}$ of the upper half plane $\mathbb{H} = \{z \in \mathbb{C} : \operatorname{Im} z > 0\}$ to $\mathbb{C}$. It can be shown that j is analytic and surjective. As for injectivity, we have the following result: if $\tau_1 \equiv \tau_2 \bmod \mathrm{SL}_2(\mathbb{Z})$, i.e. if $\tau_1 = \frac{a\tau_2 + b}{c\tau_2 + d}$ with $a, b, c, d \in \mathbb{Z}$ such that $ad - bc = 1$, then

$$\begin{pmatrix} 1 \\ \tau_1 \end{pmatrix} = \frac{1}{c\tau_2 + d} \begin{pmatrix} d & c \\ b & a \end{pmatrix},$$

hence $\mathbb{Z} + \tau_1\mathbb{Z} = \frac{1}{c\tau_2 + d}(\mathbb{Z} + \tau_2\mathbb{Z})$, and this implies $j(\tau_1) = j(\tau_2)$. It can be shown that the converse is also true: $j(\tau_1) = j(\tau_2)$ implies that $\tau_1 \equiv \tau_2 \bmod \mathrm{SL}_2(\mathbb{Z})$ (see [3]).

2.3 Endomorphisms

If $L = M$ then the endomorphisms of $\mathbb{C}/L$ correspond to $\lambda \in \mathbb{C}$ such that $\lambda L \subseteq L$. The associated $\wp$-function therefore enjoys properties which come from the structure of an algebraic variety. More exactly we have

Proposition 2.1. *If $\lambda L \subseteq L$, then*

i) λ is a rational integer or an algebraic integer in an imaginary quadratic number field;

ii) $\wp_L(\lambda z)$ is a rational function of $\wp_L(z)$ such that the degree of the numerator is λ^2 if $\lambda \in \mathbb{Z}$, and $N\lambda$ if λ is imaginary quadratic; the degree of the denominator is $\lambda^2 - 1$ and $N\lambda - 1$, respectively.

Proof. i) If $L = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ contains λL, then

$$\begin{cases} \lambda\omega_1 = a\omega_1 + b\omega_2 \\ \lambda\omega_2 = c\omega_1 + d\omega_2 \end{cases}$$

with $a, b, c, d \in \mathbb{Z}$. This implies

$$\frac{\omega_1}{\omega_2} = \frac{a\frac{\omega_1}{\omega_2} + b}{c\frac{\omega_1}{\omega_2} + d},$$

or, by putting $\tau = \omega_1/\omega_2$: $c\tau^2 + (d-a)\tau - b = 0$.

If λ is not a rational integer, then $c \neq 0$, and τ is a quadratic imaginary number (imaginary, since ω_1/ω_2 cannot be real). Since $\lambda = c\tau + d$, we get $\lambda^2 - (a+d)\lambda + ad - bc = 0$; this shows that λ is an integer in $\mathbb{Q}(\tau)$.

ii) For $\omega \in L$, we have $\wp(\lambda(z+\omega)) = \wp(\lambda z + \lambda\omega) = \wp(\lambda z)$, since $\lambda L \subseteq L$. Hence $\wp(\lambda z)$ is an elliptic function for L, and it is even (since $\wp$ is). Moreover, for $\ell \in \frac{1}{2}L$, we find $\wp(\lambda(\ell - z)) = \wp(\lambda(\ell + z))$, so if ℓ is a zero or a pole its order is even.

Let S be a set of representatives modulo L for the set of poles and zeros of $\wp(\lambda z)$; we put $S_2 = S \cap \frac{1}{2}L$. For $\beta \in S_2$, the number $n_\beta = \mathrm{ord}(\wp(\lambda z), \beta)$ is even. If $\beta \in S \setminus S_2$ we also have $-\beta \in S \setminus S_2$, and we can write $S \setminus S_2$ as a disjoint union $S_+ \cup S_-$, where $z \in S_+$ mod L if and only if $-z \in S_-$ mod L.

Now write $n_\alpha = \mathrm{ord}(\wp(\lambda z), \alpha)$ for all $\alpha \in \mathbb{C}$. The order of $\wp(\lambda z)$ in $z = 0$ is -2, hence

$$2\sum_{\alpha \in S_+} n_\alpha + \sum_{\alpha \in S_2} n_\alpha - 2 = 0.$$

Now put

$$f(z) = \prod_{\alpha \in S_+} (\wp(z) - \wp(\alpha))^{n_\alpha} \prod_{\alpha \in S_2} (\wp(z) - \wp(\alpha))^{n_\alpha/2}.$$

Then f is an elliptic function for the lattice L:

$$\begin{cases} \text{for } \alpha \in S_+, & \operatorname{ord}(f,\alpha) = n_\alpha = \operatorname{ord}(\wp(\lambda z),\alpha), \\ \text{for } \alpha \in S_2, & \operatorname{ord}(f,\alpha) = n_\alpha = \operatorname{ord}(\wp(\lambda z),\alpha), \\ \text{for } \alpha \in L, & \operatorname{ord}(f,\alpha) = \sum_{\alpha\in S_+} 2n_\alpha + \sum_{\alpha \in S_2} n_\alpha = \operatorname{ord}(\wp(\lambda z),\alpha). \end{cases}$$

Thus f has the same poles and zeros as $\wp(\lambda z)$, and we conclude that $\wp(\lambda z) = c \cdot f(z)$ for some $c \in \mathbb{C}$. Now f is a rational function in $\wp(z)$; if M and N denote the degree of numerator and denominator, then we have

$$\begin{cases} M = & \sum_{\alpha\in Z_+} n_\alpha + \sum_{\alpha\in Z_2} \frac{1}{2} n_\alpha \\ N = & \sum_{\alpha\in P_+} n_\alpha - \sum_{\alpha\in P_2} \frac{1}{2} n_\alpha, \end{cases}$$

where $S_+ = Z_+ \cup P_+$, $S_2 = Z_2 \cup P_2$, and where Z denotes the zeros and P the poles. We find

$$M - N = \sum_{\alpha\in S_+} n_\alpha + \sum_{\alpha \in S_2} \frac{1}{2} n_\alpha = 1.$$

We can also easily calculate the number of distinct poles of $\wp(\lambda z)$:

$$\alpha \in P \text{ if and only if } \lambda\alpha \in L, \text{ i.e. } \alpha \in \frac{1}{\alpha} L,$$

hence the number of poles is $\#(\frac{1}{\lambda}L/L) = (L : \lambda L)$, that is, λ^2 if $\lambda \in \mathbb{Z}$ and $N(\lambda)$ otherwise, and each of these poles is a double pole.

The number of poles of $\wp(\lambda z)$ counted with multiplicity is therefore $2(M - N) + 2N = 2N + 2$, and this concludes the proof. □

If $\frac{\omega_1}{\omega_2}$ is imaginary quadratic, the set of λ such that $\lambda L \subseteq L$ is an order in $K = \mathbb{Q}(\tau)$: it is the endomorphism ring of L. We are particularly interested in the case where this order is the ring of integers $\mathcal{O}_K$ of K, that is, the case where L is an ideal in $\mathcal{O}_K$.

Conversely, if $K = \mathbb{Q}(\tau)$ is an imaginary quadratic number field, then to each order $\mathcal{O}$ of K there exists an elliptic curve E such that $\operatorname{End}(E) = \mathcal{O}$, for example the curve $E = \mathbb{C}/\mathcal{O}$. We say that E is an elliptic curve with *complex multiplication.*

For $\mathcal{O} = \mathcal{O}_K$ we have $\operatorname{End}(E) = \mathcal{O}_K$ whenever $E = \mathbb{C}/\mathfrak{a}$, where $\mathfrak{a}$ is an ideal in $\mathcal{O}_K$; since $\mathfrak{a} \sim \mathfrak{b}$ if and only if the corresponding curves are isomorphic, we see that there exist h non-isomorphic curves with $\operatorname{End}(E) = \mathcal{O}_K$, where h is the class number of K. We conclude that we also have $(\mathbb{Q}(j(\tau) : \mathbb{Q}) \leq h$ (see [4]).

2.4 Automorphisms

They correspond to λ such that $\lambda L = L$; if the curve does not have complex multiplication, then $\lambda = \pm 1$ are the only such λ; if the curve has CM and if $\operatorname{End}(E) = \mathcal{O}$ is the maximal order in $K = \mathbb{Q}(\tau)$, then the automorphisms correspond to the units of $\mathcal{O} = \mathcal{O}_K$. Dirichlet's unit theorem asserts that the only units in $\mathcal{O}_K$ are the roots of unity contained in K (since K is imaginary quadratic), and this group is $\{\pm 1\}$ except for the following two cases:

1) $K = \mathbb{Q}(i)$: here the roots of unity are ± 1 and $\pm i$. $\mathcal{O} = \mathcal{O}_K = \mathbb{Z}[i]$ is the only order of K possessing units different from ± 1, and $\mathcal{O}$ is the endomorphism ring of the curve $E = \mathbb{C}/\mathbb{Z}[i]$. For the lattice $L = \mathbb{Z}[i]$ we find $g_3(L) = 0$ (observe that $g_3(L) = g_3(iL) = i^{-6}g_3(L)$ since $iL = L$), hence $j(L) = j(i) = 1728g_2^3/g_2^3 = 1728$ does not depend on g_2. Thus all curves $y^2 = 4x^3 - g_2x$ are isomorphic. If one chooses $g_2 = 4$, one has $y^2 = 4x^3 - 4x = 4x(x-1)(x+1)$; if $M = \omega_1(\mathbb{Z} \oplus i\mathbb{Z})$ is the corresponding lattice, then it is known that $\omega_1 = 2\int_1^\infty \frac{dt}{\sqrt{4t^3-4t}}$. This gives

$$\omega_1 = \int_1^\infty \frac{dt}{\sqrt{t^3 - t}} = \frac{\Gamma(\frac14)^2}{2\sqrt{2\pi}}.$$

This number is the lemniscatic constant ω. We deduce that $g_2(\mathbb{Z}[i]) = 4\omega^4$, hence we get

$$\sum_{(m,n)\neq(0,0)} \frac{1}{(m+in)^4} = \frac{1}{15}\frac{\Gamma(\frac14)^8}{2^6\pi^2}.$$

2) $K = \mathbb{Q}(\rho)$, where $\rho = e^{2\pi i/3}$: here the roots of unity are ± 1, $\pm\rho$ and $\pm\rho^2$. $\mathcal{O} = \mathcal{O}_K = \mathbb{Z}[\rho]$ is the only order of K possessing units different from ± 1, and $\mathcal{O}$ is the endomorphism ring of the curve $E = \mathbb{C}/\mathbb{Z}[\rho]$. For the lattice $L = \mathbb{Z}[\rho]$ we find $g_2(L) = 0$ (since $g_2(\rho L) = \rho^{-4}g_2(L)$), hence $j(\rho) = 0$ does not depend on g_3, and all the curves $y^2 = 4x^3 - g_3$ are isomorphic. If one chooses $g_3 = 4$, one gets $y^2 = 4x^3 - 4$. Let $M = \omega_1(\mathbb{Z} \oplus \rho\mathbb{Z})$ be the corresponding lattice; then we find

$$\omega_1 = 2\int_1^\infty \frac{dt}{\sqrt{4t^3 - 4}} = \frac{\Gamma(\frac13)^3}{2^{4/3}\pi},$$

from which we deduce that

$$\sum_{(m,n)\neq(0,0)} \frac{1}{(m+\rho n)^6} = \frac{\Gamma(\frac13)^{18}}{2^8\pi^6}.$$

These formulas can be generalized: if K is an imaginary quadratic number field with an order $\mathcal{O}$, and if E is an elliptic curve with complex multiplication by $\mathcal{O}$, then the corresponding lattice L determines a vector space $L \otimes \mathbb{Q}$ which is invariant under the action of K and thus has the form $L \otimes \mathbb{Q} = K \cdot \Omega$ for some $\Omega \in \mathbb{C}^\times$ defined up to elements of $K^\times$. In particular, if $\mathcal{O} = \mathcal{O}_K$, then Ω is given by the formula of Chowla-Selberg:

$$\Omega = \alpha\sqrt{\pi} \prod_{\substack{0<a<d \\ (a,d)=1}} \Gamma\Big(\frac{a}{d}\Big)^{w\varepsilon(a)/4h}.$$

Here

α is an element of $\overline{\mathbb{Q}}$;

w is the number of roots of unity in K;

h is the class number of K;

ε is the Dirichlet character modulo d;

d is the discriminant of K.

Thus, for $y^2 = 4x^3 - 4x$, one gets $\omega = \alpha\sqrt{\pi}\Gamma(\frac{1}{4})\Gamma(\frac{3}{4})$, which is in agreement with the formula given above.

3 Examples of curves with complex multiplication

Let K be a complex quadratic number field, $\mathcal{O}_K = \mathbb{Z}[\omega]$ its ring of integers. For determining the curves with complex multiplication by $\mathcal{O}_K$ one can use a method described by Stark: write down a 'sufficiently long' part of the Laurent expansion of $\wp(z)$, then compute $\wp(\omega z)$ and express it by $\wp(z)$ ([4]):

$$\begin{aligned}\wp(z) &= \frac{1}{z^2} + 3G_2 z^2 + \dots,\\ \wp(\omega z) &= \frac{1}{\omega^2 z^2} + 3G_2\omega^2 z^2 + \dots\end{aligned}$$

Now write

$$\wp(\omega z) = \frac{1}{\omega^2}\wp(z) + A(z).$$

Now we compute $\frac{1}{A}$ and proceed similarly, and get a development of $\wp(\omega z)$ as a continued fraction. We write down this series tu sufficient precision (cf. the proposition); more exactly, if $|N\omega| = m$ then we have to develop $\wp(z)$ to the order $4m - 2$ to be able to express the relation which shows us that the curve has complex multiplication by ω.

For example, if $|N\omega| = 2$, we write $\wp(z)$ to the order 6:

$$\begin{aligned}\wp(z) &= \frac{1}{z^2} + 3G_2 z^2 + 5G_3 z^4 + 7G_4 z^6 + \dots\\ \wp(\omega z) &= \frac{1}{\omega^2 z^2} + 3G_2\omega^2 z^2 + 5G_3\omega^4 z^4 + 7G_4\omega^6 z^6 + \dots\\ &= \frac{1}{\omega^2}\wp(z) + 3G_2(\omega^2 - \omega^{-2})z^2 + 5G_3(\omega^4 - \omega^{-2})z^4 + 7G_4(\omega^6 - \omega^{-2})z^6\\ &= \frac{1}{\omega^2}\wp(z) + A(z)\end{aligned}$$

Thus

$$\begin{aligned}
A &= 3G_2(\omega^2-\omega^{-2})z^2\left[1+\frac{5G_3(\omega^4-\omega^{-2})}{3G_2(\omega^2-\omega^{-2})}z^2+\frac{7G_4(\omega^6-\omega^{-2})}{3G_2(\omega^2-\omega^{-2})}z^4+\dots\right]\\
&= az^2\Big[1-a_1z^2-a_2z^4-\dots\Big]\\
\frac{1}{A} &= \frac{1}{a}\cdot\frac{1}{z^2}\Big[1+a_1z^2+(a_2+a_1^2)z^4+\dots\Big]\\
&= \frac{1}{a}\wp(z)+\frac{a_1}{a}+\frac{1}{a}(a_2+a_1^2-3G_2)z^2+\dots
\end{aligned}$$

So if there is complex multiplication by ω with $N\omega=2$, then we must have $a_2+a_1^2=3G_2$, hence

$$\frac{1}{A}=\frac{1}{a}\wp(z)+\frac{a_1}{a}$$

and

$$\wp(\omega z)=\frac{\omega^{-2}\wp(z)^2+a_1\omega^{-2}\wp(z)+a}{\wp(z)+a_1}.$$

It is convenient to take $y^2=4x^3-g_2x-g_3$ with $g_2=g_3=g$, which implies that $7G_3=3G_2$; the relation $a_2+a_1^2=3G_2$ then takes the form

$$G_2=\frac{1}{a_4+5}\Big(\frac{5a_6}{7s_4}\Big)^2 \quad \text{where} \quad s_n=\omega^n-1,$$

hence

$$g=\frac{60}{a_4+5}\Big(\frac{5a_6}{7s_4}\Big)^2.$$

First example: $K=\mathbb{Q}(\sqrt{-2})$, $\omega=i\sqrt{-2}$, $s_4=3$, $a_6=-9$, $g=\frac{3^3 5^3}{2\cdot 7^2}$, hence

$$j=\frac{1728g}{g-27}=20^3=8000.$$

The function $\wp$ is associated to an ideal class of $\mathcal{O}_K$; since $h=1$ we have $L\sim\mathcal{O}_K$, but we can also remark that, since j has only one possible value, we necessarily have $h=1$.

$$\wp_L(\omega z)=\frac{-\frac{1}{2}\wp_L(z)^2-\frac{15}{14}\wp_L(z)-\frac{3^4\cdot 5^2}{2^4\cdot 7^2}}{\wp_L(z)+\frac{15}{7}}.$$

If $L=\lambda\mathcal{O}_K$ we have

$$\lambda^4 g_2(\mathcal{O}_K)=g=\lambda^6 g_3(\mathcal{O}_K),$$

and in particular

$$g_2(\mathcal{O}_K)^3=\frac{15^3}{2\cdot 7^2}g_3(\mathcal{O}_K)^2.$$

Second example: $K=\mathbb{Q}(\sqrt{-7})$: here $\mathcal{O}_K=\mathbb{Z}\oplus\mathbb{Z}\omega$ with $\omega=\frac{1+i\sqrt{7}}{2}$ and $N\omega=2$. We find $g=\frac{5^3}{7}$ and $j=(-15)^3=-3375$, hence $h=1$.

This method seems to be of limited use; for example, with $K = \mathbb{Q}(\sqrt{-5})$ and $\omega = \sqrt{-5}$ we would have to compute $\wp(z)$ to order 18 and would have to invert four series. Nevertheless, here the class number is $h = 2$, and there are two curves such that $\mathrm{End}\,(E) = \mathbb{Z}[\sqrt{-5}]$; their modular invariants can be computed and turn out to equal (see [5])

$$j(\mathcal{O}_K) = (50 + 26\sqrt{5})^3, \quad j(\mathfrak{a}) = (50 - 26\sqrt{5})^3.$$

4 The Main Theorem of Complex Multiplication

We have seen that for $K = \mathbb{Q}(\sqrt{-d})$ there are $h(K)$ non-isomorphic elliptic curves E such that $\mathrm{End}\,(E) = \mathcal{O}_K$. If $C_1, \ldots, C_h$ are the ideal classes, then it is quite easy to see that the values $j(C_1), \ldots, j(C_h)$ are conjugated algebraic numbers of degree $\leq h$; on the other hand it is more delicate to show that these numbers are distinct and algebraic integers of degree h.

Theorem 4.1. *i) $H = K(j(C_i))$ does not depend on i; the values $j(C_i)$ are conjugated over K, and H is the Hilbert class field of K (the maximal unramified abelian extension of K; it has degree $(H : K) = h(K)$).*
ii) There exists a bijection between the ideal class group G of K and the Galois group of H/K; this bijection is in fact an isomorphism given by $\mathfrak{a} \longmapsto \sigma_{\mathfrak{a}} \in \mathrm{Gal}\,(H/K)$, where $\sigma_{\mathfrak{a}}(j(C_i)) = j([\mathfrak{a}]^{-1}C_i)$.
iii) $j(\mathfrak{a})$ is real if and only if $\mathfrak{a}$ has order dividing 2 in G; in particular, $j(\mathcal{O}_K)$ is real, and $(\mathbb{Q}(j(\mathcal{O}_K)) : \mathbb{Q}) = h$.

It is also possible to describe the maximal abelian extension of K; it is given by adjoining all elements

$$\tau\Big(\frac{1}{n}(a\omega_1 + b\omega_2)\Big), \ a, b \in \mathbb{Z}, n \in \mathbb{N}$$

to the Hilbert class field H of K. Here the function τ is defined as follows: let e be the order of $\mathrm{End}\,(\mathcal{O}_K)$ (thus e is almost always 2, and sometimes 4 or 6). One defines $g^{(e)}$ by

$$g^{(2)} = 2^7 3^5 g_2 g_3 \Delta^{-1}; \quad g^{(4)} = 2^8 3^4 g_2^2 \Delta^{-1}; \quad g^{(6)} = 2^9 3^6 g_3 \Delta^{-1}.$$

Now one puts

$$\tau(u) = (-\wp(u))^{e/2} g^{(e)}.$$

If one gives the weight 2 to $\wp$, 4 to g_2 and 6 to g_3, then τ is homogeneous of weight 0; this justifies taking $g_2 g_3 \wp \Delta^{-1}$. But if $g_2 g_3 = 0$, one has to take $g_2^2 \wp \Delta^{-1}$ if $g_3 = 0$, and $g_3 \wp^3 \Delta^{-1}$ if $g_2 = 0$. The function τ only depends on j and not on g_2 or g_3 (see e.g. Lang, Elliptic functions, Theorem 7, p. 20).

References

[1] S. Chowla, *Remarks on class-invariants and related topics*, Seminar on Complex Multiplication, Lecture Notes Math. **21**, Springer Verlag 1957

[2] G. Shimura, *Automorphic functions and Number Theory*, Lecture Notes Math. **54**, Springer Verlag 1968

[3] S. Lang, *Elliptic Curves, Diophantine Analysis*, Springer Verlag 1978

[4] H.M. Stark, *Class numbers of complex quadratic fields*, Modular Functions one Variable I, Lecture Notes Math. **320**, 153–174; Springer Verlag 1973

[5] E. Reyssat, M.F. Vigneras, *Courbes elliptiques*, Notes du cours de B. Gross à l'Université de Paris 7 (1980–1981)