Introduction to Complex Multiplication

François Morain
LIX, École polytechnique

April 10, 1995

[summary by Eithne Murray]

Abstract

The concept of complex multiplication is defined, after some background is given on elliptic functions and quadratic forms. Applications to the class number problem, primality proving and Ramanujan's formulas for $1/\pi$ are presented.

1. Introduction

This is an introduction to the ideas of complex multiplication of lattices and elliptic curves. The theory plays an important role in class field theory, and has had recent applications in algorithmic number theory, especially in elliptic curve primality proving. This presentation is a first glimpse of a very rich and deep theory developed by Kronecker, Weber, Hilbert, Shimura, Deligne, etc [3]. A good introduction to the ideas presented here is [6].

First, some background material on elliptic functions and quadratic numbers is given. This background then allows us to define complex multiplication. Some theorems that demonstrate how these three areas are interconnected and some applications in primality proving, the class number problem and Ramanujan's $1/\pi$ formulas are presented.

2. Elliptic Functions

A *lattice* is an additive subgroup L of $\mathbb{C}$ generated by two complex numbers ω_1 and ω_2 which are linearly independent over $\mathbb{R}$. We write $L = [\omega_1, \omega_2]$. An *elliptic function* for L is a function $f(z)$ meromorphic on $\mathbb{C}$ that is doubly periodic: $f(z + \omega_i) = f(z)$ for $i = 1, 2$.

One of the most important elliptic functions is the Weierstrass $\wp$-function, defined for a lattice L as

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

Let G_k, $k \geq 2$, be the *Eisenstein series* for L:

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

Then expanding $\wp(z)$ and $\wp'(z)$ near the origin, we get

$$\wp(z) = 1/z^2 + 3z^2 G_4 + 5z^4 G_6 + \cdots,$$
$$\wp'(z) = -2/z^3 + 6z G_4 + 20 z^3 G_6 + \cdots.$$

Define $g_2 = 60G_4$ and $g_3 = 140G_6$. Then $\wp$ satisfies the differential equation

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

In addition, $\wp$ and $\wp'$ are generators for the field of elliptic functions over L. One of the main theorems of complex multiplication states when we can write $\wp(\alpha z)$ as a rational function in $\wp(z)$.

In order to easily detect the difference between lattices that are complex multiples of each other and lattices that are truly different, we introduce the concept of j-invariant of a lattice.

For a lattice $L = [\omega_1, \omega_2]$, define $\tau = \omega_2/\omega_1$. Then let $\Delta(\tau) = g_2^3(\tau) - 27g_3^2(\tau)$. The *$j$-invariant* of L is the complex number

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

It turns out that two lattices are isomorphic if and only if they have the same j-invariant.

The j-invariant can also be used to classify elliptic curves [8]. Consider the elliptic curve E, which is an equation of the form $y^2 = 4x^3 - g_2x - g_3$. From the theory of elliptic curves, we know there is a unique lattice L_E such that $g_2 = g_2(L_E)$ and $g_3 = g_3(L_E)$. (The inverse is also true - given a lattice L over $\mathbb{C}$, there is a unique corresponding elliptic curve E_L). We extend the definition of j to elliptic curves by saying that $j(E) = j(L_E)$. Then two elliptic curves E_1, E_2 are isomorphic if and only if $j(E_1) = j(E_2)$.

3. Quadratic Forms

One application of complex multiplication is in solving the class number problem, which is a problem related to quadratic forms. Some background on quadratic forms is needed in order to state this problem. A *quadratic form* is a function $f(x, y) = ax^2 + bxy + cy^2$ with $a, b, c \in \mathbb{Z}$, and its *discriminant* is $-D = b^2 - 4ac$. For future reference, define the *discriminant of a quadratic number* τ to be the discriminant of the unique quadratic form $(a, b, c), a > 0, (a, b, c) = 1$ such that τ is the root of $ax^2 + bx + c = 0$.

Define $Q(-D)$ to be the set of all quadratic forms with discriminant $-D$ and $(a, b, c) = 1$. Associate with f a matrix $A = \left(\begin{smallmatrix} a & b/2 \\ b/2 & c \end{smallmatrix}\right)$. Then two quadratic forms f, f' are *equivalent* if there is a matrix $M \in SL_2(\mathbb{Z})$ such that $A' = M^{-1}AM$.

Define $H(-D) = Q(-D)/\sim$, where $\sim$ is the equivalence relation defined above. Then an important theorem states that $h(-D) = |H(-D)|$ is finite. Each class contains exactly one form which is *reduced* ($|b| \leq a \leq c$, and $b \geq 0$ if $|b| = a$ or $a = c$), and we identify each class with this form: $H(-D) = \{Q_1, Q_2, \ldots, Q_h\}$. Then, there is a (fairly complicated) way of *composing* two forms, and this operation makes $H(-D)$ into an abelian group. $H(-D)$ is called the *class group*, and $h(-D)$ is the *class number*. The problem is to find all $-D$ for which $h(-D)$ is fixed, especially for $h(-D) = 1$. See [7].

4. Complex Multiplication

For two lattices L and M, we say that $L \sim M$ if and only if $\exists \alpha \in \mathbb{C}$ such that $\alpha L = M$. Define $S(L) = \{\alpha \in \mathbb{C}, \alpha L \subset L\}$.

Finally, we can give our definition of complex multiplication.

Definition 1. If $S(L)$ contains more than $\mathbb{Z}$, L is said to have *complex multiplication*. If α is in $S(L) - \mathbb{Z}$, L has *complex multiplication by* α.

$S(L)$ has some special properties.

Theorem 1. *Let $L = [\omega_1, \omega_2]$. Then $\alpha \in S(L), \alpha \in \mathbb{C} - \mathbb{Z}$ if and only if α is a quadratic integer.*

Writing $\tau = \omega_2/\omega_1$, then $\alpha = a\tau + b$, $\tau \notin \mathbb{R}$, so $\mathbb{Q}(\alpha) = \mathbb{Q}(\tau) = \mathbb{Q}(\sqrt{-D})$, where $-D$ is the discriminant of the quadratic number τ. Denote this field by K.

Quadratic field theory tells us that the ring of integers of K is $\mathcal{O}_K = \mathbb{Z}[(-D + \sqrt{-D})/2]$. Then $S(L)$ is a subring of $\mathcal{O}_K$. Thus, if L has complex multiplication by a single element α, then it has complex multiplication by each member of a ring of elements in an imaginary quadratic field. Note that the non-integer elements of $S(L)$ are genuinely complex, which explains the name complex multiplication.

EXAMPLE. Let $Q = (a, b, c) \in H(-D)$, and set $\tau_Q = (-b + \sqrt{-D})/(2a)$. Then the lattice $L_Q = [1, \tau_Q]$ has complex multiplication by all of $\mathcal{O} = \mathbb{Z}[(-D + \sqrt{-D})/2]$.

One remarkable fact is the relationship between lattices with complex multiplication and the $\wp$ function.

THEOREM 2. *Let L be a lattice, and $\wp$ be the $\wp$-function for L. Then L has complex multiplication by $\alpha \in \mathbb{C} - \mathbb{Z}$ if and only if*

$$\wp(\alpha z) = F(\wp(z))/G(\wp(z))$$

with F, G relatively prime polynomials, and $\deg(F) = \deg(G) + 1 = N(\alpha)$.

Algorithms exist to find F and G [6].

Complex multiplication can also be defined on elliptic curves, in the obvious way.

DEFINITION 2. An elliptic curve E has *complex multiplication* if and only if the associated lattice L has.

The following theorem shows which E_Q have complex multiplication, and by what ring.

THEOREM 3. *All elliptic curves $E_Q = \mathbb{C}/L_Q$, where L_Q is defined as in the example, have complex multiplication by the full ring of integers $\mathcal{O}$. These are the only ones with complex multiplication by $\mathcal{O}$, up to isomorphism.*

The following theorem relates complex multiplication with the j-invariant.

THEOREM 4. *Let E be an elliptic curve with complex multiplication, L its associated lattice, and D the associated discriminant. Then $j(E)$ is an algebraic integer of degree $h(-D)$.*

THEOREM 5. *The minimal polynomial of $j(\tau_Q)$, known as the* class equation, *is*

$$H_{-D}(X) = \prod_{Q \in H(-D)} (X - j(\tau_Q))$$

If K is an imaginary quadratic field, then $K_H = K(j(\tau_Q))$ is Galois and is called the Hilbert class field of K.

5. Applications

5.1. ECPP. Elliptic Curve Primality Proving makes use of the class equation to find large prime numbers. Part of the method is to determine if, for a prime p, (p) splits completely in K_H, or equivalently, $H_{-D}(X)$ has h roots mod$p$. Thus one of the problems is to actually compute the class equation. One algorithm to do this involves the theory of complex multiplication [2].

5.2. Class Number Problem. We would like to be able to calculate the number of $-D$'s that have class number h, as well as determine what those $-D$'s are. Work done from 1934 onwards has solved the problem for $h = 1, 2, 3, 4$ and $5 \leq h \leq 23$ for h odd [7, 1].

One method is to consider the minimal polynomial of $j(\tau)$ which has degree $h = h(-D)$. If we can find the minimal polynomial, then its degree will tell us the class number h for the $-D$ associated with τ. The following theorem supplies one approach to the problem.

THEOREM 6. *Let $\gamma_2(z) = \sqrt[3]{j(z)}$ sending $i\mathbb{R}$ to $\mathbb{R}$. If $3 \not| D$ then $\mathbb{Q}(\gamma_2(\tau)) = \mathbb{Q}(j(\tau))$.*

Thus, finding the degree of the minimal polynomial of γ_2 will give the degree of $j(z)$, and hence $h(-D)$. This is an easier task than working with $j(z)$ directly. Various other rather complicated functions (Weber functions [9]) are used in the development of this problem. In particular, the Weber functions allow us to find all imaginary quadratic fields of class number 1.

THEOREM 7. *$h(-D) = 1$ if and only if $d = 3, 4, 7, 8, 11, 19, 43, 67, 163$.*

5.3. Ramanujan. Recalling the Eisenstein series, define E_k by $G_k = 2\zeta(k)E_k$, and then define

$$s_2 = \left(E_2(\tau) - \frac{3}{\pi \Im(\tau)}\right) \frac{E_4(\tau)}{E_6(\tau)}.$$

Then Ramanujan proved

THEOREM 8. *If $\tau \in K$, then $s_2 \in K_H$.*

When combined with an identity from Fricke and Clausen involving s_2, D and $j(\tau)$, some very complicated identities involving π are produced, including the following when $D = 163$:

$$\sum_{n=0}^{\infty} (c_1 + n) \frac{(6n)!}{(3n)!n!^3} \frac{(-1)^n}{640320^{3n}} = \frac{(640320)^{3/2}}{163 \cdot 8 \cdot 27 \cdot 11 \cdot 19 \cdot 127} \frac{1}{\pi}$$

where $c_1 = 13591409/(163 \cdot 2 \cdot 9 \cdot 7 \cdot 11 \cdot 19 \cdot 127)$. This series gives a very fast-converging approximation for $1/\pi$. Other values of D produce similar formulas. See [4] and [5] for more details.

Bibliography

[1] Arno (S.), Robinson (M. L.), and Wheeler (F. S.). – Imaginary quadratic fields with small odd class number. – December 1993. Preprint.

[2] Atkin (A. O. L.) and Morain (François). – Elliptic curves and primality proving. *Mathematics of Computation*, vol. 61, n° 203, July 1993, pp. 29–68.

[3] Borel (A.), Chowla (S.), Herz (C. S.), Iwasawa (K.), and Serre (J.-P.). – *Seminar on complex multiplication.* – Springer, 1966, *Lecture Notes in Mathematics.*

[4] Borwein (Jonathan M.) and Borwein (Peter B.). – More Ramanujan-type series for $1/\pi$. In Andrews (G. E.), Askey (R. A.), Berndt (B. C.), Ramanathan (K. G.), and Rankin (R. A.) (editors), *Ramanujan revisited.* pp. 359–374. – Academic Press, 1988.

[5] Chudnovsky (D. V.) and Chudnovsky (G. V.). – Approximations and complex multiplication according to Ramanujan. In Andrews (G. E.), Askey (R. A.), Berndt (B. C.), Ramanathan (K. G.), and Rankin (R. A.) (editors), *Ramanujan revisited.* pp. 375–472. – Academic Press, 1988.

[6] Cox (David A.). – *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication.* – John Wiley & Sons, New York, 1989.

[7] Goldfeld (Dorian). – Gauss' class number problem for imaginary quadratic fields. *Bulletin of the American Mathematical Society*, vol. 13, n° 1, July 1985, pp. 23–37.

[8] Silverman (J. H.). – *Advanced Topics in the Arithmetic of Elliptic Curves.* – Springer-Verlag, 1994, *Graduate Texts in Mathematics*, vol. 151.

[9] Weber (H.). – *Lehrbuch der Algebra.* – Chelsea Publishing Company, New York, 1902, vol. I, II, III.