Rev.R.Acad.Cienc.Exact.Fis.Nat. (Esp)
Vol. 94, N.º 3, pp 333-338, 2000
Monográfico: Contribuciones al estudio algorítmico de problemas de moduli aritméticos

COMPLEX MULTIPLICATION POINTS ON MODULAR CURVES

(complex multiplication point/modular curve/quadratic form/modular polynomial/class polynomial)

A. Arenas*, P. Bayer**

* Facultat de Matemàtiques, Universitat de Barcelona, Gran Vía de les Corts Catalanes, 585. E-08007 Barcelona (arenas@mat.ub.es)

** Facultat de Matemàtiques, Universitat de Barcelona, Gran Vía de les Corts Catalanes, 585. E-08007 Barcelona (bayer@mat.ub.es)

Abstract

In this paper we generalise the concept of complex multiplication points on the modular curve $X_0(N)$ to the case of any discriminant D. We show how to reduce their study and evaluation of their number to that of primitive $\mathcal{O}$-ideals of type $\alpha\mathcal{O}$ with the norm $n(\alpha)$ equal to N, where $\mathcal{O}$ is the order of discriminant D of a quadratic field and, ultimately, to that of the primitive representations of N by the principal form of discriminant D. When $D < 0$, explicit computations are exhibited.

Resumen

En este artículo, damos una generalización del concepto de puntos con multiplicación compleja de la curva modular $X_0(N)$, para cualquier discriminante D. Reducimos su estudio y la evaluación de su número al de los $\mathcal{O}$-ideales primitivos $\alpha\ \mathcal{O}$ de norma $n(\alpha)$ igual a N, donde $\mathcal{O}$ es el orden de discriminante D de un cuerpo cuadrático y, en última instancia, al de las representaciones primitivas de N por la forma principal de discriminante D. El caso $D <$ 0 se ilustra con cálculos explícitos.

Introduction

In this paper we consider a special type of Heegner triplets, called complex multiplication triplets, essentially according to Mazur **[Ma 77]** for the case of complex multiplication points on the modular curve $X_0(N)$. They are associated to an order $\mathcal{O}$ of discriminant D of a quadratic field. In the sequel, these complex multiplication points will simply be called of type (N, D). Complex multiplication points of type (N, D) are easily seen to be described by the set of triplets $(\mathcal{O}, \alpha\mathcal{O}, [\mathfrak{a}])$, where $\alpha\mathcal{O}$ is a principal $\mathcal{O}$-ideal of norm N and $[\mathfrak{a}]$ stands for the class in $\mathrm{Pic}^+(\mathcal{O})$ of the invertible fractional $\mathcal{O}$-ideal $\mathfrak{a}$. This set of triplets is shown to be in one-to-one correspondence with the $\Gamma_0(N)$-classes of primitive integral binary quadratic forms of discriminant D admitting representatives $aNX^2 + bXY + cY^2$ which are $\mathbf{SL}(2, \mathbb{Z})$-equivalent to $aX^2 + bXY + cNY^2$. This result allows us to compute the number of complex multiplication points of type (N, D). We illustrate the methods used with a table and examples. Throughout the paper we keep the notations and definitions of **[Ar-Ba 2000-1]**.

1. COMPLEX MULTIPLICATION POINTS ON $X_0(N)$

As in **[Ar-Ba 2000-1]**, we fix an integer $N > 1$ and a discriminant D (positive or negative).

Definition 1.1. *A complex multiplication triplet* $(\mathcal{O}, \alpha\mathcal{O}, [\mathfrak{a}])$ *of type* (N, D) *is given by an order* $\mathcal{O}$ *of discriminant D of a quadratic field, an element* $\alpha \in \mathcal{O}$ *of positive norm N satisfying that the quotient* $\mathcal{O}/\alpha\mathcal{O}$ *is a cyclic group, and an element* $[\mathfrak{a}]$ *of* $Pic^+(\mathcal{O})$.

In other words, a complex multiplication triplet of type (N, D) is a Heegner triplet $(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])$ of type (N, D), where $\mathfrak{n}$ is a principal $\mathcal{O}$-ideal generated by an element of positive norm.

In our next considerations we will show why this definition is consistent with the usual concept of complex multiplication point on the modular curve.

Recall that the complex points $Y_0(N)(\mathbb{C})$ of the open modular curve $Y_0(N)$ have the structure of a Riemann surface analytically isomorphic to the quotient space $\mathbb{H}/\Gamma_0(N)$. Let $X_0(N)$ be the natural compactification of $Y_0(N)$. Modifying slightly Mazur's definition **[Ma 77]**, we give the following geometric description of a complex multiplication point.

Definition 1.2. *Given an order* $\mathcal{O} = \mathcal{O}_D$ *of discriminant* $D = D_0 r^2$ *in the imaginary quadratic field of discriminant* D_0*, a Heegner point* $y = (E_1 \rightarrow E_2)$ *in* $Y_0(N)(\mathbb{C})$ *is called a complex multiplication point of type* (N, D) *if*

[1] Partially supported by DGES: PB96-0166.

$E_1 = E_2 =: E$ and the endomorphism ring End(E) is isomorphic to $\mathcal{O}$.

The following propositions give conditions which will guarantee the existence of complex multiplication points of type (N, D).

Proposition 1.3. *Given an order $\mathcal{O} = \mathcal{O}_D$ in an imaginary quadratic field, the modular curve $Y_0(N)$ has complex multiplication points of type (N, D) if and only if there exists a principal primitive $\mathcal{O}$-ideal $\mathfrak{n}$ of norm N.*

Proof. We write $E = \mathbb{C}/\mathfrak{a}$, where the lattice $\mathfrak{a}$ is assumed to be an invertible fractional $\mathcal{O}$-ideal, and bearing in mind that the endomorphisms of $\mathbb{C}/\mathfrak{a}$ (passing to the universal covering space $\mathbb{C}$) are given by multiplications by complex numbers α such that $\alpha\mathfrak{a} \subseteq \mathfrak{a}$, i. e., by $\alpha \in \mathcal{O}$. The kernel of such an isogeny of order N (if $\alpha \neq 0$) is obviously $\alpha^{-1}\mathfrak{a}/\mathfrak{a}$. But, by **[Ar-Ba 2000-1** lemma 1.4], $\alpha^{-1}\mathfrak{a}/\mathfrak{a} \simeq \mathcal{O}/\alpha\mathcal{O}$. □

Remark 1.4. *If we adopt in definition 1.2 and proposition 1.3 the exact point of view of* **[Ar-Ba 2000-1]** *instead of considering here $E_1 = E_2$ (= $\mathbb{C}/\mathfrak{a}$ say), we should consider $E_2 = \mathbb{C}/\mathfrak{a}$ and $E_1 = \mathbb{C}/\alpha\mathfrak{a}$ if we want the map $E_1 \longrightarrow E_2$ to be induced by the identity from $\mathbb{C}$ to $\mathbb{C}$, rather than being multiplication by α. By virtue of* [**Ar-Ba 2000-1** lemma 1.4], *we realise that this entails no essential difference. But we think that the definition as it stands is more convenient in the present paper.*

Definition 1.5. *Given an order $\mathcal{O}$ of, positive or negative, discriminant $D = D_0r^2$, we consider the $\mathbb{Z}$-basis of $\mathcal{O}$ given by (1, $r\omega$), where*

$$\omega = \begin{cases} \sqrt{\dfrac{D_0}{4}} & \text{if } D_0 \equiv 0 \pmod 4, \\ \dfrac{-1+\sqrt{D_0}}{2} & \text{if } D_0 \equiv 1 \pmod 4. \end{cases}$$

The principal form of discriminant D is

$$f_D(X,Y) = \begin{cases} X^2 - \dfrac{D}{4}Y^2 & \text{if } D \equiv 0 \pmod 4, \\ X^2 + XY + \left(\dfrac{1-D}{4}\right)Y^2 & \text{if } D \equiv 1 \pmod 4. \end{cases}$$

The normic form of discriminant D, $(X - Yr\omega)(X - Yr\omega')$, where ω' stands for the conjugate of ω, is equal to

$$n_D(X, Y) = \begin{cases} X^2 - \dfrac{D}{4}Y^2 & \text{if } D_0 \equiv 0 \pmod 4, \\ X^2 + XY + r^2\left(\dfrac{1-D_0}{4}\right)Y^2 & \text{if } D_0 \equiv 1 \pmod 4. \end{cases}$$

For any discriminant D, the principal form has the property of being a representative of the unit class in the group $H(D)$ of $\mathbf{SL}(2, \mathbb{Z})$*-equivalence classes of primitive integral binary quadratic forms of discriminant D.*

Lemma 1.6. *A primitive binary quadratic form of discriminant D is a representative of the unit class in $H(D)$ if and only if it represents 1. In particular, the normic form lies in the unit class.*

Proof. Let $f(X, Y)$ be a primitive binary quadratic form which represents 1. Then f is $\mathbf{SL}(2, \mathbb{Z})$-equivalent to a primitive form of the type $X^2 + bXY + \left(\dfrac{b^2 - D}{4}\right)Y^2$ (cf. the proof **[Za 81** Satz 1, § 8, p. 60]) The following equalities

$$\begin{bmatrix} 1 & 0 \\ \frac{b}{2} & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & \frac{-D}{4} \end{bmatrix}\begin{bmatrix} 1 & \frac{b}{2} \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & \frac{b}{2} \\ \frac{b}{2} & \frac{b^2-D}{4} \end{bmatrix}$$

if $D \equiv 0$ (mod 4); and

$$\begin{bmatrix} 1 & 0 \\ \frac{b-1}{2} & 1 \end{bmatrix}\begin{bmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & \frac{1-D}{4} \end{bmatrix}\begin{bmatrix} 1 & \frac{b-1}{2} \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & \frac{b}{2} \\ \frac{b}{2} & \frac{b^2-D}{4} \end{bmatrix}$$

if $D \equiv 1$ (mod 4), show that $f(X, Y)$ is $\mathbf{SL}(2, \mathbb{Z})$-equivalent to the principal form in both cases. □

Proposition 1.7. *Given an order $\mathcal{O}$ of, positive or negative, discriminant D and an integer $N \geq 1$, there exists a principal primitive ideal $\mathfrak{n} \subseteq \mathcal{O}$ of norm N generated by an element of positive norm if and only if the unit class in $H(D)$ represents N primitively.*

Proof. Assume that the ideal $\mathfrak{n}$ satisfying $\mathfrak{n} \subseteq \mathcal{O}$, $\mathcal{O}/\mathfrak{n} \simeq \mathbb{Z}/N\mathbb{Z}$, is principal, i. e., $\mathfrak{n} = \alpha\mathcal{O}$, with $\alpha \in \mathcal{O}$ having positive norm $n(\alpha)$. Then, $N = n(\mathfrak{n}) = n(\alpha)n(\mathcal{O}) = \text{n}(\alpha)$, so that the normic form n_D represents N, but it remains to be shown that α yields a primitive representation of N. By the theory of elementary divisors, there exists a $\mathbb{Z}$-basis (ξ, η) of $\mathcal{O}$ such that

$$\mathfrak{n} = \langle \xi, \mathrm{N}\eta \rangle \subset \mathcal{O} = \langle \xi, \eta \rangle;$$

and, in particular, the coordinates of ξ in any $\mathbb{Z}$-basis of $\mathcal{O}$ are coprime. But $\xi \in \alpha\mathcal{O}$, so that, for some $\rho \in \mathcal{O}$, $\xi = \alpha\rho$. Now, write this equality in terms of the usual basis (1, $r\omega$) of $\mathcal{O}$. If $\alpha = s + tr\omega$, $\xi = p + qr\omega$ and $\rho = u + vr\omega$, then

$$p + qr\omega = \xi = (s + tr\omega)(u + vr\omega) =$$

$$= su + tvr^2\omega^2 + (sv + tu)r\omega.$$

Now consider the two cases

$$\omega^2 = \begin{cases} \dfrac{D_0}{4} & \text{if } D_0 \equiv 0 \pmod{4}, \\[2ex] -\omega - \dfrac{1-D_0}{4} & \text{if } D_0 \equiv 1 \pmod{4}. \end{cases}$$

separately. In the first case, we have

$$p = su + tvr^2\,\frac{D_0}{4}, \qquad q = sv + tu,$$

and, in the second,

$$p = su - tvr^2\,\frac{1-D_0}{4}, \qquad q = sv + tu - tvr^2,$$

so, in either case, gcd $(s, t) = 1$, since gcd $(p, q) = 1$.

Conversely, if the normic form represents N primitively, then there exists an element $\alpha \in \mathcal{O} = \langle 1, r\omega\rangle$ such that $n(\alpha) = N$ and $\alpha = x - yr\omega$ with $\gcd(x, y) = 1$. The primitivity of α implies that there exists $\beta \in \mathcal{O}$ such that (α, β) is a $\mathbb{Z}$-basis of $\mathcal{O}$. Obviously, $\alpha\mathcal{O}$ is principal and $n(\alpha\mathcal{O}) = N$. Moreover, by the theory of elementary divisors, we know that there exists a $\mathbb{Z}$-basis (ξ, η) of $\mathcal{O}$ and integers s, t such that $(s\xi, st\eta)$ is a $\mathbb{Z}$-basis of $\alpha\mathcal{O}$, but if $s > 1$, α would not be primitive, so $s = 1$, $\mathcal{O} = \langle \xi, \eta\rangle$, $\alpha\mathcal{O} = \langle \xi, t\eta\rangle$ and $t = N = n(\alpha\mathcal{O})$. Thus $\mathcal{O}/\alpha\mathcal{O}$ is cyclic. □

Let us recall that the group $\Gamma_0(N)$ acts on the set $\mathcal{H}(N, D)$ of integral quadratic forms of type $aNX^2 + bXY + cY^2$ with $b^2 - 4Nac = D$ and $\gcd(aN, b, c) = \gcd(a, b, cN) = 1$. If $\mathcal{O}$ stands for the unique quadratic order of discriminant D, then the quotient $H(N, D) = \mathcal{H}(N, D)/\Gamma_0(N)$, which is a finite set, is in one-to-one correspondence with the set of pairs $(\mathfrak{n}, [\mathfrak{a}])$, where $\mathfrak{n}$ is a primitive $\mathcal{O}$-ideal of norm N and $[\mathfrak{a}]$ is the proper class of an invertible fractional $\mathcal{O}$-ideal $\mathfrak{a}$ (see **[Ar-Ba 2000-1]** thm. 3.4]).

In what follows we are interested in the subset of this latter set where $\mathfrak{n}$ is $\mathcal{O}$-principal generated by a primitive element of positive norm. Then we have, with our previous notations, the following

Theorem 1.8. *Given a quadratic order $\mathcal{O}$ of discriminant D, the set of pairs $(\alpha\mathcal{O}, [\mathfrak{a}])$, where $n(\alpha) = N$ and $\alpha\mathcal{O}$ is primitive, is in one-to-one correspondence with the subset of classes of $H(N, D)$ defined by representatives $aNX^2 + bXY + cY^2$ which are* **SL**$(2, \mathbb{Z})$*-equivalent to $aX^2 + bXY + cNY^2$.*

Proof. We refer to the proof of **[Ar-Ba 2000-1]** thm. 3.4] and keep the same notations used there. To begin with, consider the restriction to the subset $\{(\alpha\mathcal{O}, [\mathfrak{a}])\}$ of the map constructed from the set $\{(\mathfrak{n}, [\mathfrak{a}])\}$ into $H(N, D)$. Now, if $\mathfrak{n} = \alpha\mathcal{O}$ with $n(\alpha) = N$, as $\mathfrak{a} = \omega_1\langle 1, \tau\rangle$ and $\mathfrak{n}^{-1}\mathfrak{a} = \alpha^{-1}\mathfrak{a} = \frac{\omega_1}{N}\langle 1, N\tau\rangle$ are, obviously, properly equivalent, we see that $\langle 1, \tau\rangle$ and $\langle 1, N\tau\rangle$ are, also, properly equivalent. As both $(1, \tau)$ and $(1, N\tau)$ are oriented bases, we conclude that $N\tau$ is **SL**$(2, \mathbb{Z})$-equivalent to τ. In other words, $aX^2 + bXY + cNY^2$ is **SL**$(2, \mathbb{Z})$-equivalent to $aNX^2 + bXY + cY^2$. Conversely, let $aNX^2 + bXY + cY^2$ of discriminant D be **SL**$(2, \mathbb{Z})$-equivalent to $aX^2 + bXY + cNY^2$. Then the respective roots τ and $N\tau$, of the corresponding dehomogenised equations such that both $(1, \tau)$ and $(1, N\tau)$ are oriented bases, are **SL**$(2, \mathbb{Z})$-equivalent, i. e., $\langle 1, \tau\rangle$ and $\langle 1, N\tau\rangle$ yield the same element of $\mathrm{Pic}^+(\mathcal{O})$ and it only remains to be shown that $\langle 1, \tau\rangle\langle 1/N, \tau\rangle^{-1}$ is principal and generated by an element of positive norm. In fact, as $\langle 1, \tau\rangle = \rho\langle 1, N\tau\rangle$ with $n(\rho) > 0$, we have $\langle 1, \tau\rangle\langle 1/N, \tau\rangle^{-1} = \rho\langle 1, N\tau\rangle(1/N\langle 1, N\tau\rangle)^{-1} = \rho N\mathcal{O}$, and, obviously, $n(\rho N) > 0$; actually $n(\rho N) = N$. □

Corollary 1.9. *The number $c(N, D)$ of complex multiplication points of type (N, D) is*

$$c(N, D) = \frac{r^*(N, f_D)}{o^+(D)}\, h^+(D).$$

Proof. Since $h^+(D) = \#\mathrm{Pic}^+(\mathcal{O})$, we only have to count the number of primitive ideals $\alpha\mathcal{O}$ with $n(\alpha) = N$. To this end recall first that α and β both of positive norm generate the same $\mathcal{O}$-ideal if and only if α and β differ by a multiplicative factor of $\mathcal{O}$ of norm 1. Now, each generator α of positive norm of a primitive principal ideal of $\mathcal{O}$ of norm N yields, according to the proof of proposition 1.7, a primitive representation of N by f_D. But every element of the form $\varepsilon\alpha$, with ε a unit of $\mathcal{O}$ of norm 1, obviously yields an $\mathbf{O}^+(D)$-equivalent representation of N, where $\mathbf{O}^+(D)$ stands for the group of proper automorphisms of f_D and, conversely, as a consequence of **[Ar-Ba 2000-1]** lemma 3.2]. The result follows. □

2. THE KRONECKER CONGRUENCE

In this section we review some properties of the elliptic modular function j. An element τ in the upper halfplane $\mathbb{H}$ is called imaginary quadratic, over $\mathbb{Q}$, if it satisfies an integral quadratic equation $a\tau^2 + b\tau + c = 0$ with $a, b, c \in \mathbb{Z}$ and $\gcd(a, b, c) = 1$. We shall denote $D(\tau) = D = b^2 - 4ac < 0$ the discriminant of τ.

Theorem 2.1. (cf. **[We 08]**, **[Si 49]**) *Let τ be a complex algebraic number in $\mathbb{H}$.*

i) If τ is not quadratic imaginary, then the value $j(\tau)$ is transcendental.

ii) If τ is quadratic imaginary of discriminant D, then the value $j(\tau)$ is an algebraic integer of degree $h(D)$ over $\mathbb{Q}$. *In this case, the value $j(\tau)$ is called a singular modulus. In particular, if $h(D) = 1$ then $j(\tau) \in \mathbb{Z}$.*

One of the most remarkable properties of singular moduli is the following:

Theorem 2.2. (cf. **[We 08]**) *Let $\mathcal{O}$ be an imaginary quadratic order of discriminant D. For each* **SL**$(2, \mathbb{Z})$*-reduced primitive positive binary quadratic form of discriminant D, $a_iX^2 + b_iXY + c_iY^2$, let τ_i be the root belonging to $\mathbb{H}$ of the quadratic equation $a_iX^2 + b_iX + c_i = 0$, for $1 \le i \le h(D)$. Then the class polynomial associated to $\mathcal{O}$,*

$$H_D(X) = \prod_{i=1}^{h(D)} (X - j(\tau_i)),$$

is an integral irreducible polynomial of degree $h(D)$.

Let $\Gamma(1) := \mathbf{SL}(2, \mathbb{Z})$. For fixed $N > 1$, let $\psi(N) = N\Pi_{p|N}\left(1 + \frac{1}{p}\right)$ and let α_i, for $1 \le i \le \psi(N)$, stand for the $\psi(N)$ distinct integral matrices $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$, such that, $ad = N$, $a > 0$, $0 \le b < d$, and $\gcd(a, b, d) = 1$ (see **[La 73** Ch. 5 § 1]). Then, we have the following equalities:

$$\{\alpha \in \mathbf{GL}(2, \mathbb{Z}) \mid \alpha \text{ primitive}, \det(\alpha) = N\} =$$
$$= \Gamma(1)\begin{bmatrix} N & 0 \\ 0 & 1 \end{bmatrix}\Gamma(1) = \bigcup_{\substack{ad = N,\\ 0 \le b < d,\\ \gcd(a,b,d)=1}} \Gamma(1)\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} =$$
$$= \bigcup_{i=1}^{\psi(N)} \Gamma(1)\alpha_i \quad \text{(disjoint)}.$$

We consider the polynomial

$$F_N(X) := \prod_{i=1}^{\psi(N)} (X - j \circ \alpha_i) \in \mathbb{Z}[j][X],$$

where $j(\alpha_i(z)) := j\left(\frac{az + b}{d}\right)$. We may consider $F_N(X) = F_N(j, X) \in \mathbb{Z}[j, X]$ as a polynomial in two independent variables. $F_N(j, X)$ is called the modular polynomial of level N. The equation $F_N(j, X) = 0$ is the modular equation of level N. We recall its main properties in the following:

Theorem 2.3 (cf. **[La 73], [We 08]**)

i) *$F_N(j, X)$ is irreducible over $\mathbb{C}(j)$ and has degree $\psi(N)$.*

ii) *$F_N(j, X)$ is symmetrical in j and X, i. e., $F_N(j, X) = F_N(X, j)$.*

iii) *If N is a prime number, then $F_N(X, X) \in \mathbb{Z}[X]$, and its leading term is $-X^{2N}$.*

We point out that the minus sign in the third item is missing in **[La 73]**.

The main relationship between the class polynomial and the modular polynomial is given by the so-called Kronecker congruence.

Theorem 2.4. (cf. **[We 08]**) *Let f_D be the principal form of discriminant $D < 0$. Then*

$$F_N(X, X) = \pm \prod_D H_D(X)^{t(N, D)}, \quad \textit{where}$$

$$t(N, D) := \frac{r^*(N, f_D)}{o^+(D)}.$$

In particular, one obtains the Kronecker-Hurwitz class number relation:

$$deg\ F_N(X, X) = \sum_D c(N, D).$$

We point out that the $c(N, D) = h^+(D)t(N, D)$ different complex multiplication points of type (N, D) in $\mathbb{H}/\Gamma_0(N)$ exactly produce $h^+(D)$ different points on $X_0(N)(\mathbb{C})$.

In table 1 we list all possible discriminants $D < 0$, for $3 \le N \le 11$, which give complex multiplication points of type (N, D), as well as their number $c(N, D)$. The following proposition illustrates the calculation of complex multiplication points in the case $N = 11$.

Proposition 2.5. *Let $N = 11$. The exact values of $D < 0$ for which there exist complex multiplication points of type $(11, D)$ are:*

$$D = -7, -7 \cdot 2^2, -8, -11, -11 \cdot 2^2, -19, -35, -40, -43.$$

The corresponding values to the four $\Gamma_0(11)$-inequivalent complex multiplication points of the upper half-plane for $D = -35$ may be given by

$$\tau_1 = \frac{-19 + \sqrt{-35}}{22}, \quad \tau_2 = \frac{-19 + \sqrt{-35}}{66},$$
$$\tau_3 = \frac{-3 + \sqrt{-35}}{22}, \quad \tau_4 = \frac{-25 + \sqrt{-35}}{110}.$$

Proof. In fact, given a discriminant $D \equiv 0 \pmod 4$, there exist complex multiplication points of type $(11, D)$ if and only if the principal form $f_D = X^2 - \frac{D}{4}Y^2$ represents

Table 1

N	D	$c(N, D)$
3	-3	1
	$-12 = -3 \cdot 2^2$	1
	-8	2
	-11	2
	other values	0
5	-4	2
	$-16 = -4 \cdot 2^2$	2
	-11	2
	-19	2
	-20	2
	other values	0
7	-3	2
	$-12 = -3 \cdot 2^2$	2
	$-27 = -3 \cdot 3^2$	2
	-7	1
	$-28 = -7 \cdot 2^2$	1
	-19	2
	-24	4
	other values	0
11	-7	2
	$-28 = -7 \cdot 2^2$	2
	-8	2
	-11	1
	$-44 = -11 \cdot 2^2$	3
	-19	2
	-35	4
	-40	4
	-43	2
	other values	0

11 primitively. This condition is verified for the discriminants $D = -7 \cdot 2^2, -8, -11 \cdot 2^2, -40$.

Now, if $D \equiv 1 \pmod 4$, then there exist complex multiplication points of type $(11, D)$ if and only if the principal form $X^2 + XY + \frac{1-D}{4}Y^2$ represents 11 primitively. This condition is verified for the discriminants $D = -7, -11, -19, -35, -43$. Observe that, in this case, if $D < -43$, we have $f_D = \left(X + \frac{1}{2}Y\right)^2 - \frac{D}{4}Y^2 > \left(X + \frac{1}{2}Y\right)^2 + \frac{43}{4}Y^2$.

Let us now show representatives of the four $\Gamma_0(11)$-inequivalent complex numbers $\tau_1, \dots, \tau_4$ in the upper half-plane, corresponding to the complex multiplication points of type $(11, -35)$ (cf. thm. 1.8). First of all, observe that there are two principal primitive ideals of norm 11 in $\mathbb{Q}(\sqrt{-35})$, i. e., $t(11, -35) = 2$, namely, $\alpha_1\mathcal{O}$, $\alpha_2\mathcal{O}$, where $\alpha_1 = \frac{3+\sqrt{-35}}{2}$, $\alpha_2 = \frac{3-\sqrt{-35}}{2}$, and $\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z}\left(\frac{1+\sqrt{-35}}{2}\right)$. We take as representatives of the two $\mathbf{SL}(2, \mathbb{Z})$-classes of forms in $\mathbb{Q}(\sqrt{-35})$:

$$X^2 + XY + 9Y^2, \quad 3X^2 + XY + 3Y^2.$$

They are in one-to-one correspondence with the classes in $\mathrm{Pic}^+\mathcal{O}$ of invertible fractional $\mathcal{O}$-ideals

$$\mathfrak{a}_1 = \left\langle 1, \frac{-1+\sqrt{-35}}{2} \right\rangle, \qquad \mathfrak{a}_2 = \left\langle 1, \frac{-1+\sqrt{-35}}{6} \right\rangle.$$

Then, recall that we have the complex multiplication points $(\alpha_i\mathcal{O}, [\mathfrak{a}_j])$ for $1 \le i \le 2$ and $1 \le j \le 2$. We will detail the calculations of $(\alpha_2\mathcal{O}, [\mathfrak{a}_1])$. We have

$$\alpha_2^{-1}\mathfrak{a}_1 = \left\langle \frac{3+\sqrt{-35}}{22}, \frac{-19+\sqrt{-35}}{22} \right\rangle.$$

Now we search for an $\omega_1 \in \mathfrak{a}_1$, i. e.,

$$\omega_1 = \lambda + \mu\left(\frac{-1+\sqrt{-35}}{2}\right), \qquad \gcd(\lambda, \mu) = 1,$$

such that $\omega_1/11 \in \alpha_2^{-1}\mathfrak{a}_1$. We can take $\omega_1 = \frac{3+\sqrt{-35}}{2}$ and can complete to a $\mathbb{Z}$-basis of $\mathfrak{a}_1$ with $\omega_2 = -1$. Then

$$\tau = \omega_2/\omega_1 = \frac{-3+\sqrt{-35}}{22}.$$

Of course, the different choices in our previous selections yield different possibilities for τ which, however, are $\Gamma_0(11)$-equivalent in accordance with thm. 1.8. Moreover, it is easy to check that the points τ_1 and τ_3 are $\mathbf{SL}(2, \mathbb{Z})$-equivalents, and τ_2 and τ_4, too. In fact, (cf. **[Ka-Yu 91]**):

$$F_{11}(X, X) = H_{-7}(X)^2 H_{-8}(X)^2 H_{-11}(X) H_{-19}(X)^2 H_{-28}(X)^2$$
$$H_{-35}(X)^2 H_{-40}(X)^2 H_{-43}(X)^2 H_{-44}(X),$$

with $H_{-35}(X) = X^2 + 2^{19} \cdot 3^2 \cdot 5^2 X - 2^{30} \cdot 5^3$. □

REFERENCES

1. **[Ar-Ba 2000-1]** Arenas, A. & Bayer, P. (2000), Heegner points on modular curves, *Rev. R. Acad.-Cienc. Exact. Fis. Nat., Esp.* **94**, 323-332.
2. **[Bo-Sh 66]** Borevich, Z. I. & Shafarevich, I. R. (1966), *Number Theory,* Academic Press.

3. **[Ka-Yu 91]** Kaltofen, E. & Yui, N. (1991), Explicit construction of the Hilbert class fields of imaginary quadratic fields by integer lattice reduction, in the book *Number Theory, New York Seminar 1989-90,* D. V. Chudnovsky et al., ed. Springer, pp. 149-202.

4. **[La 73]** Lang, S. (1973), *Elliptic Functions,* Addison & Wesley.

5. **[Ma 77]** Mazur, B. (1977), Modular Curves and the Eisenstein Ideal, *Publ. Math. IHES* **47**, 33-186.

6. **[We 08]** Weber, H. (1962), *Lehrbuch der Algebra, Bd. III,* Vieweg, 1908. Chelsea.

7. **[Za 81]** Zagier, D. B. (1981), *Zetafunktionen und quadratische Körper,* Hochschultext, Springer.