

JACOBI THETANULLWERTE, PERIODS OF ELLIPTIC CURVES AND MINIMAL EQUATIONS

JORDI GUÀRDIA

ABSTRACT. We introduce a family of modular functions which provide the coefficients of algebraic Weierstrass equations for complex toruses corresponding to elliptic curves defined over a number field. The equations built with these new modular functions have good arithmetical properties, since they are minimal global equations outside 2 and 3.

Introduction

The relation between elliptic curves and complex toruses has been studied mainly by means of the Weierstrass \wp -function. The relations of theta-functions with elliptic curves are well-known, although their arithmetical applications have been less explored. We want here to exploit the properties of the theta functions to find Weierstrass equations of elliptic curves with good arithmetic properties.

Every complex torus \mathbb{C}/Λ has an associated elliptic curve

$$E_\Lambda : Y^2 = 4X^3 - g_2(\Lambda)X - g_3(\Lambda),$$

where $g_2(\Lambda) = 60 \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^4}$, $g_3(\Lambda) = 140 \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^6}$. The curve is defined over the field generated by the j -invariant

$$j(\Lambda) = 1728 \frac{g_2(\Lambda)^3}{g_2(\Lambda)^3 - 27g_3(\Lambda)^2},$$

by the equation

$$Y^2 + XY = X^3 - \frac{36}{j(\Lambda) - 1728}X - \frac{1}{j(\Lambda) - 1728},$$

whose coefficients will not be integral over $\mathbb{Z}[j(\Lambda)]$ in general. Moreover, one of the coefficients $g_2(\Lambda), g_3(\Lambda)$ of the first equation may be algebraically independent from $j(\Lambda)$. The Weierstrass \wp function and its derivative establish an analytic isomorphism $\varphi : \mathbb{C}/\Lambda \rightarrow E_\Lambda(\mathbb{C})$ between the torus and the elliptic curve such that $\varphi^*dX/2Y = dz$. Hence, the period lattice spanned by the differential form $dX/2Y$ is precisely Λ .

Received March 21, 2003.

2000 *Mathematics Subject Classification.* 11GF11, 11G05, 14K25.

Key words and phrases. Thetanullwerte, elliptic curves, periods, minimal equations.

Partially supported by MCYT BFM2000-0627, BFM2003-06768-C02-02.

Reciprocally, given an elliptic curve in general Weierstrass form

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6,$$

integrating the differential form $\omega_E = \frac{dX}{2Y+a_1X+a_3}$ along the non-trivial closed continuous paths on E , we obtain a period lattice Λ_E such that the complex torus \mathbb{C}/Λ_E is analytically isomorphic to the original curve.

Through these two correspondences, isomorphic elliptic curves go to homothetic lattices and viceversa. For this reason, it is common to work only with lattices of the form $\Lambda = \langle 1, \tau \rangle$, where τ is an element of the Poincaré upper half plane $\mathbb{H} = \{z \in \mathbb{C} \mid \text{Im}(z) > 0\}$. The corresponding objects are then denoted as depending only on τ : $g_2(\tau), g_3(\tau), j(\tau), E_\tau$, etc.

While this reduction is very useful for many purposes, it seems to cause a loss of arithmetic information. For instance, the period lattice of the elliptic curve

$$Y^2 = 4X^3 - 4X$$

can be taken to be $\Lambda = \mathbb{Z}[i]$, but $g_2(\mathbb{Z}[i]) = 189.07272\dots$, which has nothing to do with the coefficient of X in the equation of the curve. If one wants to recover the original curve, one has to re-scale the lattice and take $\Omega\mathbb{Z}[i]$, where $\Omega = \sqrt{\pi}\Gamma(1/4)/\Gamma(3/4)$. Given τ such that $j(\tau) \in \overline{\mathbb{Q}}$, it is a difficult matter to determine a scaling factor $u \in \mathbb{C}$ such that the values $u^4g_2(\tau), u^6g_3(\tau)$ are algebraic. This article is concerned with the resolution of this problem.

In the general set up of abelian varieties, this problem was first studied by Shimura ([8]), who introduced certain scaling factors expressed in terms of derivatives of theta functions. Several authors ([3], [5], [4]) have studied these factors from different viewpoints. As we will see, the case of elliptic curves is quite easier and it can be solved independently from Shimura's work. The link between our solution and Shimura's ideas is provided by the triple product formula of Jacobi (formula (2) below).

Two classical formulas of Jacobi will allow us to obtain intrinsic arithmetic information from a given τ :

$$\sqrt{k} = \frac{\theta_2(\tau)}{\theta_3(\tau)}, \quad K = \frac{\pi}{2}\theta_3(\tau)^2,$$

expressing the modulus k and the complete elliptic integral of the first kind $K(k) = \int_0^1 \frac{dx}{\sqrt{(1-x^2)(1-k^2x^2)}}$ in terms of *Thetanullwerte* (defined below), that is, in terms of values at zero of theta functions. The first equality provides an efficient way of computing absolute invariants for a complex torus $\mathbb{C}/\langle 1, \tau \rangle$. The second formula can be seen as a relation between the holomorphic differential form dz on the complex torus \mathbb{C}/Λ and the differential form $\frac{dx}{\sqrt{(1-x^2)(1-k^2x^2)}}$ on the elliptic curve.

By a combined application of Jacobi's formulas, we provide an answer to the following two questions:

- A) Given a complex torus $\mathbb{C}/\langle 1, \tau \rangle$ such that the associated elliptic curve E_τ is defined over a number field, determine a Weierstrass equation for E_τ with algebraic coefficients.
- B) Given an elliptic curve E over an order in a field of characteristic different from 2,3 with potentially good reduction, find a (quasi) minimal equation for it.

The solution of the first problem is based on the use of Thetanullwerte, but could be also derived with no mention to them. The formulas obtained are universal, in the sense that they remain valid over an arbitrary field, and hence we can use them to solve the second problem.

1. Basic facts about theta functions

We recall some basic facts about theta functions, which we will need along the article. First of all, we remind the definition of the four one-dimensional theta functions. Given $a, b \in \{0, 1/2\}$, we define:

$$\begin{aligned}\theta(z, \tau) &= \sum_{n \in \mathbb{Z}} \exp(\pi i \tau n^2 + 2\pi i n z) \\ \theta_{a,b}(z, \tau) &= \exp(\pi i a^2 \tau + 2\pi i a(z + b)) \theta(z + b + a\tau, \tau) \\ &= \sum_{n \in \mathbb{Z}} \exp(\pi i \tau (n + a)^2 + 2\pi i (n + a)(z + b)).\end{aligned}$$

We write as usual

$$\begin{aligned}\theta_1(z, \tau) &= \theta_{1/2, 1/2}(z, \tau), & \theta_2(z, \tau) &= \theta_{1/2, 0}(z, \tau), \\ \theta_3(z, \tau) &= \theta_{0, 0}(z, \tau), & \theta_4(z, \tau) &= \theta_{0, 1/2}(z, \tau).\end{aligned}$$

We are specially interested in the values at $z = 0$ of these functions, $\theta_k(0, \tau)$, which are usually called *Thetanullwerte* and denoted by $\theta_k(\tau)$. Since $\theta_1(z, \tau)$ is an odd function of z , $\theta_1(\tau)$ is identically zero, and we consider instead the value $\theta'_1(\tau) := \frac{\partial \theta_1(z, \tau)}{\partial z} \big|_{z=0}$. Jacobi proved two fundamental relations between the Thetanullwerte:

$$\begin{aligned}(1) \quad & \theta_2(\tau)^4 + \theta_4(\tau)^4 = \theta_3(\tau)^4, \\ (2) \quad & \theta'_1(\tau) = -\pi \theta_2(\tau) \theta_3(\tau) \theta_4(\tau).\end{aligned}$$

Moreover, they have the following modular behaviour:

$$\begin{aligned}\theta_2(\tau + 1) &= \zeta_8 \theta_2(\tau), & \theta_2(-1/\tau) &= \zeta_8^{-1} \sqrt{\tau} \theta_4(\tau), \\ \theta_3(\tau + 1) &= \theta_4(\tau), & \theta_3(-1/\tau) &= \zeta_8^{-1} \sqrt{\tau} \theta_3(\tau), \\ \theta_4(\tau + 1) &= \theta_3(\tau), & \theta_4(-1/\tau) &= \zeta_8^{-1} \sqrt{\tau} \theta_2(\tau).\end{aligned}$$

where $\zeta_8 = \exp(\pi i/4)$, and $\sqrt{\tau}$ denotes the principal branch of the square root. We refer to [7, ch. I], for proofs of all these formulas.

2. Periods of algebraic differential forms

Let E be an elliptic curve defined over the complex numbers. Let $L = \mathbb{Q}(j_E)$ be its field of definition. We may think that E is given by an equation $Y^2 = (1 - X^2)(1 - k^2 X^2)$ over a certain extension $L(k)$ of L . The period lattice corresponding to this model of E is determined by the complete integrals of the first kind $K(k), K'(k)$ (cf. [6, chap. 2]):

$$K(k) = \int_0^1 \frac{dx}{\sqrt{(1-x^2)(1-k^2x^2)}},$$

$$K'(k) = \int_1^{1/k} \frac{dx}{\sqrt{(1-x^2)(1-k^2x^2)}} = K(\sqrt{1-k^2}).$$

We can take the normalized period lattice given by $\tau = iK'(k)/K(k)$ (cf. [6, p. 131]), which satisfies $j_E = j(\tau)$. The elliptic curve E and the complex torus $\mathbb{C}/\langle 1, \tau \rangle$ are analytically isomorphic, and it is clear that, through this isomorphism, the differential form $K(k)dz$ on the torus corresponds to a differential form on the curve which is defined over $L(k)$.

The modulus k and the integral $K(k)$ can be expressed in terms of the Theta-nullwerte (cf. [9]):

$$\sqrt{k} = \frac{\theta_2(\tau)}{\theta_3(\tau)}, \quad K = \frac{\pi}{2} \theta_3(\tau)^2.$$

If we depart from a given $\tau \in \mathbb{H}$, we can use these two formulas to find directly the value of $K(k)$ and hence build the differential form $K(k)dz$ with no need of an equation of the elliptic curve E_τ . In fact, combining these formulas with (1) we see that any of the differential forms on the torus $\mathbb{C}/\langle 1, \tau \rangle$:

$$\pi\theta_2(\tau)\theta_4(\tau)dz, \quad \pi\theta_2(\tau)\theta_3(\tau)dz, \quad \pi\theta_3(\tau)\theta_4(\tau)dz$$

comes from a differential form on the elliptic curve E_τ , defined over a finite extension of $L(k)$.

Definition 2.1. *We call theta-factors of the periods of E_τ the numbers:*

$$\pi_2(\tau) := \pi\theta_3(\tau)\theta_4(\tau), \quad \pi_3(\tau) := e^{\pi i/4}\pi\theta_2(\tau)\theta_4(\tau), \quad \pi_4(\tau) := \pi\theta_2(\tau)\theta_3(\tau).$$

The algebraic period lattices of E_τ are

$$\Lambda_{\tau,2} = \pi_2(\tau)\langle 1, \tau \rangle, \quad \Lambda_{\tau,3} = \pi_3(\tau)\langle 1, \tau \rangle, \quad \Lambda_{\tau,4} = \pi_4(\tau)\langle 1, \tau \rangle.$$

As a consequence of the discussion above, we know that the $\Lambda_{\tau,r}$ are period lattices of models of the elliptic curve E_τ , defined over certain algebraic extensions of $\mathbb{Q}(j(\tau))$. We shall find these algebraic models explicitly. Since we know that the period lattice spanned by the differential form $dX/2Y$ of the elliptic curve

$$(3) \quad Y^2 = 4X^3 - g_2(\Lambda_{\tau,r})X - g_3(\Lambda_{\tau,r})$$

is precisely $\Lambda_{\tau,r}$, we have to compute the invariants $g_2(\Lambda_{\tau,r}), g_3(\Lambda_{\tau,r})$, and find their relations with $j(\tau)$. We are then led to the following definition:

Definition 2.2. Let $\pi_r(\tau) = \pi\theta_s(\tau)\theta_t(\tau)$ be any theta-factor. The algebraic Eisenstein functions $\mathcal{G}_{2,r}, \mathcal{G}_{3,r}$ and the algebraic discriminants \mathcal{D}_r are:

$$\begin{aligned}\mathcal{G}_{2,r}(\tau) &= 6^2 \frac{g_2(\tau)}{\pi_r(\tau)^4} = (-1)^r 24 \left(\frac{\theta_2(\tau)^8 + \theta_3(\tau)^8 + \theta_4(\tau)^8}{\theta_s(\tau)^4 \theta_t(\tau)^4} \right), \\ \mathcal{G}_{3,r}(\tau) &= 6^3 \frac{g_3(\tau)}{\pi_r(\tau)^6} = -i^{(r-2)^2} 32 \frac{(\theta_3(\tau)^4 + \theta_4(\tau)^4)(\theta_2(\tau)^4 - \theta_4(\tau)^4)(\theta_2(\tau)^4 + \theta_3(\tau)^4)}{\theta_s(\tau)^6 \theta_t(\tau)^6}, \\ \mathcal{D}_r(\tau) &= 6^6 \frac{\Delta(\tau)}{\pi_r(\tau)^{12}} = \mathcal{G}_{2,r}(\tau)^3 - 27\mathcal{G}_{3,r}(\tau)^2 = (-1)^r 2^{10} 3^6 \frac{\theta_r(\tau)^8}{\theta_s(\tau)^4 \theta_t(\tau)^4}.\end{aligned}$$

The reasons for the term *algebraic* in this definition will become clear along the following sections.

3. Modular properties of the theta-factors

The modular transformations of the theta-functions give immediately the modular properties of the theta-factors.

Proposition 3.1. The theta-factors of the periods of E_τ satisfy the functional equations

$$\begin{aligned}\pi_2(\tau + 1) &= \pi_2(\tau), & \pi_2(-1/\tau) &= -i\tau\pi_4(\tau), \\ \pi_3(\tau + 1) &= i\pi_4(\tau), & \pi_3(-1/\tau) &= -i\tau\pi_3(\tau), \\ \pi_4(\tau + 1) &= \pi_3(\tau), & \pi_4(-1/\tau) &= -i\tau\pi_2(\tau).\end{aligned}$$

Let us denote by $S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $T = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ the usual generators of the modular group $\Gamma = \text{SL}_2(\mathbb{Z})$. We consider the following congruence subgroups: $\Gamma_2 := \Gamma_0(2) = \langle S, TS^2T \rangle$, $\Gamma_3 := \Gamma_\theta = S^{-1}T\Gamma_0(2)TS = \langle S^2, T \rangle$, $\Gamma_4 := \Gamma^0(2) = T\Gamma_0(2)T = \langle S^2, TST \rangle$.

The transformation of the theta-factors under the generators of these groups are given in the following table:

$$\begin{aligned}\pi_2(S\tau) &= \pi_2(\tau), & \pi_2(TS^2T\tau) &= -i(2\tau - 1)\pi_2(\tau), \\ \pi_3(S^2\tau) &= i\pi_3(\tau), & \pi_3(T\tau) &= -i\tau\pi_3(\tau), \\ \pi_4(S^2\tau) &= i\pi_4(\tau), & \pi_4(STS\tau) &= (\tau + 1)\pi_4(\tau).\end{aligned}$$

4. Algebraic modular forms

From the formulas above, we can deduce the modular behaviour of the algebraic Eisenstein functions.

Proposition 4.1. *We have:*

$\mathcal{G}_{2,2}(S\tau) = \mathcal{G}_{2,2}(\tau)$	$\mathcal{G}_{2,3}(S\tau) = \mathcal{G}_{2,4}(\tau)$	$\mathcal{G}_{2,4}(S\tau) = \mathcal{G}_{2,3}(\tau)$
$\mathcal{G}_{2,2}(T\tau) = \mathcal{G}_{2,4}(\tau)$	$\mathcal{G}_{2,3}(T\tau) = \mathcal{G}_{2,3}(\tau)$	$\mathcal{G}_{2,4}(T\tau) = \mathcal{G}_{2,2}(\tau)$
$\mathcal{G}_{3,2}(S\tau) = \mathcal{G}_{3,2}(\tau)$	$\mathcal{G}_{3,3}(S\tau) = -\mathcal{G}_{3,4}(\tau)$	$\mathcal{G}_{3,4}(S\tau) = \mathcal{G}_{3,3}(\tau)$
$\mathcal{G}_{3,2}(T\tau) = -\mathcal{G}_{3,4}(\tau)$	$\mathcal{G}_{3,3}(T\tau) = -\mathcal{G}_{3,3}(\tau)$	$\mathcal{G}_{3,4}(T\tau) = -\mathcal{G}_{3,2}(\tau)$
$\mathcal{D}_2(S\tau) = \mathcal{D}_2(\tau)$	$\mathcal{D}_3(S\tau) = \mathcal{D}_4(\tau)$	$\mathcal{D}_4(S\tau) = \mathcal{D}_3(\tau)$
$\mathcal{D}_2(T\tau) = \mathcal{D}_4(\tau)$	$\mathcal{D}_3(T\tau) = \mathcal{D}_3(\tau)$	$\mathcal{D}_4(T\tau) = \mathcal{D}_2(\tau)$

Let us define three systems of multipliers for the groups defined above:

$$\begin{aligned} \nu_2 : \Gamma_0(2) &\longrightarrow \{\pm 1\}, & \nu_3 : \Gamma_\theta &\longrightarrow \{\pm 1\}, & \nu_4 : \Gamma^0(2) &\longrightarrow \{\pm 1\}, \\ \nu_2(S) &= 1, & \nu_3(S^2) &= -1, & \nu_4(S^2) &= -1, \\ \nu_2(TS^2T) &= -1, & \nu_3(T) &= -1, & \nu_4(TST) &= 1. \end{aligned}$$

Corollary 4.2.

- a) $\mathcal{G}_{2,2}(\tau), \mathcal{D}_2(\tau)$ are modular functions for the group $\Gamma_0(2)$, and $\mathcal{G}_{3,2}(\tau)$ is a modular function with multiplier system ν_2 for $\Gamma_0(2)$.
- b) $\mathcal{G}_{2,3}(\tau), \mathcal{D}_3(\tau)$ are modular functions for the group Γ_θ , and $\mathcal{G}_{3,3}(\tau)$ is a modular function with multiplier system ν_3 for Γ_θ .
- c) $\mathcal{G}_{2,4}(\tau), \mathcal{D}_4(\tau)$ are modular functions for the group $\Gamma^0(2)$, and $\mathcal{G}_{3,4}(\tau)$ is a modular function with multiplier system ν_4 for $\Gamma^0(2)$.

Remark: The functions $\mathcal{G}_{3,r}$ are in fact modular functions for congruence subgroups of level 4.

We shall use these modular functions to solve the problems stated in the introduction. We begin relating them with other well-known invariants for elliptic curves.

Let Γ_r denote the three level 2 congruence subgroups corresponding to the modular functions $\mathcal{G}_{2,r}, \mathcal{G}_{3,r}, \mathcal{D}_r$. The modular curve $X_r = \Gamma_r \backslash \mathbb{H}$ has genus 0, since it is a quotient of the modular curve $X(2)$ which has also genus 0. In fact, since the three subgroups $\Gamma_2, \Gamma_3, \Gamma_4$ are conjugate, the curves X_2, X_3, X_4 are isomorphic. We have two quotient maps:

$$X(2) \longrightarrow X_r \longrightarrow X(1).$$

It is well-known that the invariant $j(\tau)$ is a *Hauptmodul* for the curve $X(1)$. Concerning the curve $X(2)$, a *Hauptmodul* for it is given by the Legendre invariant ([6, p. 131 and p. 181]):

$$(4) \quad \lambda(\tau) = k(\tau)^2 = \frac{\theta_2(\tau)^4}{\theta_3(\tau)^4}.$$

The quotient map $X(2) \longrightarrow X(1)$ sends $\lambda(\tau) \in \mathbb{C}$ to

$$(5) \quad j(\tau) = 2^8 \frac{(\lambda(\tau)^2 - \lambda(\tau) + 1)^3}{\lambda(\tau)^2(1 - \lambda(\tau))^2} = 32 \frac{(\theta_2^8(\tau) + \theta_3^8(\tau) + \theta_4^8(\tau))^3}{\theta_2^8(\tau)\theta_3^8(\tau)\theta_4^8(\tau)}.$$

We might relate the modular functions $\mathcal{G}_{2,r}, \mathcal{G}_{3,r}, \mathcal{D}_r$ with these two invariants in a number of ways. For instance, we may write the definitions of all the invariants in terms of Thetanullwerte, and eliminate these by using formula (1) above. It

is easier to find the relations with $\lambda(\tau)$, which amounts to explicit the map $X(2) \rightarrow X_r$. We present the results obtained for $\mathcal{G}_{2,3}, \mathcal{G}_{3,3}, \mathcal{D}_3$, the remaining ones being quite similar.

Proposition 4.3. *We have:*

$$\begin{aligned} \text{a) } \mathcal{G}_{2,3}(\tau) &= 48 \frac{\lambda(\tau)^2 - \lambda(\tau) + 1}{(1 - \lambda(\tau))\lambda(\tau)}, \\ \text{b) } \mathcal{G}_{3,3}(\tau) &= 32i \frac{(\lambda(\tau) + 1)(\lambda(\tau) - 2)(2\lambda(\tau) - 1)}{((1 - \lambda(\tau))\lambda(\tau))^{3/2}}, \\ \text{c) } \mathcal{D}_3(\tau) &= -\frac{2^{10}3^6}{\lambda(\tau)(1 - \lambda(\tau))}. \end{aligned}$$

From these formulas we may find the relations of the algebraic Eisenstein forms with the invariant $j(\tau)$, by eliminating the invariant $\lambda(\tau)$ using formula (5). In this case, we obtain the same relations for the three families of invariants:

Proposition 4.4. *Let $u(\tau) = j(\tau) - 1728$. Then*

$$\begin{aligned} \text{a) } \mathcal{G}_{2,r}(\tau)^3 - 3^2 j(\tau) \mathcal{G}_{2,r}(\tau) + 2^4 3^3 j(\tau) &= 0; \\ \text{b) } \mathcal{G}_{3,r}(\tau)^6 + 2^4 3 u(\tau) \mathcal{G}_{3,r}(\tau)^4 - u(\tau)^2 (j(\tau) - 2^8 3) \mathcal{G}_{3,r}(\tau)^2 + 2^{12} u(\tau)^3 &= 0. \\ \text{c) } \mathcal{D}_r(\tau)^3 + 2^{10} 3^7 \mathcal{D}_r(\tau)^2 - 2^{12} 3^{12} (j(\tau) - 2^8 3) \mathcal{D}_r(\tau) + 2^{30} 3^{18} &= 0; \end{aligned}$$

The formulas in proposition 4.4 may be seen as equations for the modular curves X_r . They have the remarkable property that all of their coefficients are integral, and all of them are powers of 2 and 3. Hence, they define the curve X_r over any field of characteristic different from 2 and 3. Moreover, we see that:

Theorem 4.5. *The invariants $\mathcal{G}_{2,r}(\tau), \mathcal{G}_{3,r}(\tau)$ and $\mathcal{D}_r(\tau)$ are algebraic integers of degree at most 3, 6 and 3 respectively over the ring $\mathbb{Z}[j(\tau)]$.*

Since $\mathcal{G}_{2,r}(\tau)$ is in fact a *hauptmodul* for the curve X_r , the invariants $\mathcal{G}_{3,r}(\tau), \mathcal{D}_r(\tau), j(\tau)$, will depend algebraically on it:

Proposition 4.6. *We have:*

$$\begin{aligned} \text{a) } 27 \mathcal{G}_{3,r}(\tau)^2 &= (\mathcal{G}_{2,r}(\tau) + 144)(\mathcal{G}_{2,r}(\tau) - 72)^2; \\ \text{b) } \mathcal{D}_r(\tau) &= 2^6 3^5 (\mathcal{G}_{2,r}(\tau) - 48); \\ \text{c) } j(\tau) &= \frac{\mathcal{G}_{2,r}(\tau)^3}{9(\mathcal{G}_{2,r}(\tau) - 48)}. \end{aligned}$$

5. Minimal equations for algebraic elliptic curves

Let E be an elliptic curve defined over a number field K . We choose a period $\tau \in \mathbb{H}$ such that $j(\tau) = j(E) \in K$ is the absolute invariant of E . By theorem 4.5, the equations

$$\mathcal{E}_r(\tau) : Y^2 = 4X^3 - \mathcal{G}_{2,r}(\tau)X - \mathcal{G}_{3,r}(\tau)$$

are algebraic integral models of $E_\tau \simeq E$, defined over the ring of integers of the field $L = K(\mathcal{G}_{2,r}(\tau), \mathcal{G}_{3,r}(\tau))$. By propositions 4.4 and 4.6, we know that the extension L/K has degree at most 6.

The following result shows the good arithmetic properties of these algebraic equations:

Theorem 5.1. *If the elliptic curve E has potentially good reduction at a prime \mathfrak{p} in K then the equations*

$$\mathcal{E}_r(\tau) : Y^2 = 4X^3 - \mathcal{G}_{2,r}(\tau)X - \mathcal{G}_{3,r}(\tau)$$

are \mathfrak{p} -integral models of E . If moreover \mathfrak{p} does not divide 2 and 3, the equations $\mathcal{E}_r(\tau)$ have good reduction at the primes of L over \mathfrak{p} .

Proof. The coefficients of the algebraic equation \mathcal{E}_r are algebraic integers over $\mathbb{Z}[j(\tau)]$ and, by hypothesis, $j(\tau)$ is \mathfrak{p} -integral. The discriminant of $\mathcal{E}_r(\tau)$ is the algebraic discriminant $\mathcal{D}_r(\tau)$, which is again an algebraic integer over $\mathbb{Z}[j(\tau)]$. By proposition 4.4, we know that the norm of $\mathcal{D}_r(\tau)$ over \mathbb{Q} is only divisible by 2 and 3, so that $\mathcal{E}_r(\tau)$ has good reduction at \mathfrak{p} when \mathfrak{p} does not divide 2 and 3. \square

As a consequence, when $j(\tau)$ is an algebraic integer, the algebraic equation $\mathcal{E}_r(\tau)$ is almost a global minimal model of E_τ , since it can only have bad reduction at primes dividing 2 and 3.

6. Examples

The algebraic equations introduced in section 4 are particularly interesting for elliptic curves with potentially good reduction everywhere, i.e., with integral j -invariant. Elliptic curves with complex multiplication constitute a good source for such curves.

Gross ([1]), using a formula of Chowla and Selberg, found a minimal model over \mathbb{Z} of the elliptic curves with complex multiplication by the ring of integers of $\mathbb{Q}(\sqrt{-p})$ for the primes $p = 7, 11, 19, 43, 67, 163$ (all of them with class number 1). While our algebraic equations are not defined over \mathbb{Z} in general, they can be used for any elliptic curve with or without complex multiplication.

For $p = 7$ and $\tau = \frac{1+\sqrt{-7}}{2}$ Gross found the equation

$$E : Y^2 + XY = X^3 - X^2 - 2X - 1,$$

with invariant $j(\tau) = -3^3 5^3$, and discriminant $\Delta = -7^3$. The equations $\mathcal{E}_r(\tau)$ provided by the algebraic Eisenstein functions are defined over quadratic extensions of \mathbb{Q} :

$$\begin{aligned} \mathcal{E}_2(\tau) : Y^2 &= 4X^3 - 45X - 27\sqrt{7}, & \mathcal{D}_2(\tau) &= -2^6 3^6, \\ \mathcal{E}_3(\tau) : Y^2 &= 4X^3 + 45\frac{1-3i\sqrt{7}}{2} - 27\frac{35-9i\sqrt{7}}{2}, & N_{K/\mathbb{Q}}\mathcal{D}_3(\tau) &= 2^{24} 3^{12}, \\ \mathcal{E}_4(\tau) : Y^2 &= 4X^3 + 45\frac{1+3i\sqrt{7}}{2} + 27\frac{35+9i\sqrt{7}}{2}, & N_{K/\mathbb{Q}}\mathcal{D}_4(\tau) &= 2^{24} 3^{12}. \end{aligned}$$

These equations are minimal models of E over $\mathbb{Z}[\sqrt{7}]$, $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ everywhere except at the primes dividing 2. Using Chowla-Selberg' formula ([2]), we may

express the values of the theta-factors in terms of values of Gamma function. For instance, we find the following identity:

$$\pi_3 \left(\frac{1 + \sqrt{-7}}{2} \right)^2 = i\pi \frac{3 + i\sqrt{7}}{28} \frac{\Gamma(1/7)\Gamma(2/7)\Gamma(4/7)}{\Gamma(3/7)\Gamma(5/7)\Gamma(6/7)}$$

Let us show an example with class number two. Let $p = 5$ and $\tau = \sqrt{-5}$. The simplest equation obtained with our algebraic Eisenstein functions is

$$\mathcal{E}_3(\tau) : Y^2 = 4X^3 + 48(35 + 16\sqrt{5})X - 128i\sqrt{44258 + 19793\sqrt{5}},$$

with $j(\tau) = 320(1975 + 884\sqrt{5})$ and $\mathcal{D}_3(\tau) = 2^{12}3^6(9 + 4\sqrt{5})$. It is defined over the field $K = \mathbb{Q}(\sqrt{\frac{\sqrt{5}-1}{2}})$. We can derive easily a global minimal equation over the ring of integers of K , by pulling out 2^4 and 2^6 from the coefficients $\mathcal{G}_{23}(\tau), \mathcal{G}_{33}(\tau)$. We thus arrive to the equation

$$Y^2 = 4X^3 + 3(35 + 16\sqrt{5})X - 2i\sqrt{44258 + 19793\sqrt{5}},$$

with discriminant $\Delta = -3^6(9 + 4\sqrt{5})$. From the formula of Chowla-Selberg we find the identity:

$$\pi_3(\sqrt{-5})^4 = -\frac{\pi^2}{400} \left(\frac{-1 + \sqrt{5}}{2} \right)^3 \frac{\Gamma(\frac{1}{20})\Gamma(\frac{3}{20})\Gamma(\frac{7}{20})\Gamma(\frac{9}{20})}{\Gamma(\frac{11}{20})\Gamma(\frac{13}{20})\Gamma(\frac{17}{20})\Gamma(\frac{19}{20})}.$$

References

- [1] Gross, B.H., *Arithmetic on Elliptic Curves with Complex Multiplication*, Lecture Notes in Mathematics, 776, Springer, 1980.
- [2] Chowla, S., and Selberg, A., ‘On Epstein Zeta-function’, J. Reine Angew. Math. **227** (1967) 86-110.
- [3] David, S., ‘Fonctions thêta et points de torsion des variétés abéliennes’, Compositio Math. **78** (1991) 121-160.
- [4] Igusa, J., ‘On Jacobi’s derivative formula and its generalizations’, Amer. J. Math. 102, 409-446, 1980.
- [5] Masser, David., and Wüstholz, G., ‘Periods and minimal abelian subvarieties’, Ann. of Math. **137** (1993) 407-458.
- [6] McKean, H., and Moll, V., *Elliptic curves: function theory, geometry, arithmetic*, Cambridge Univ. Press, 1999.
- [7] Mumford, D., *Tata lectures on theta, I*, Progress in Mathematics, 28, Birkhäuser Boston, 1983.
- [8] Shimura, G., ‘On the derivatives of theta functions and modular forms’, Duke Math. J., **44** (1977) 365-387.
- [9] Whittaker, E.T. and Watson, G.N., *A course of Modern Analysis*, 4th ed. (reprinted) Cambridge U.P., 1927.

DEPARTAMENT DE MATEMÀTICA APLICADA IV., ESCOLA POLITÈCNICA SUPERIOR
D’ENGINYERIA DE VILANOVA I LA GELTRÚ,, AVINGUDA VÍCTOR BALAGUER S/N. E-08800
VILANOVA I LA GELTRÚ

E-mail address: guardia@mat.upc.es