

## THETANULLWERTE: FROM PERIODS TO GOOD EQUATIONS

JORDI GUÀRDIA

*Abstract*

---

We will show the utility of the classical Jacobi Thetanullwerte for the description of certain period lattices of elliptic curves, providing equations with good arithmetical properties. These equations will be the starting point for the construction of families of elliptic curves with everywhere good reduction.

---

### 1. Introduction

The determination of an equation for an elliptic curve associated to a given complex torus is a common task in number theory. The common solution follows from the uniformization of the torus by means of the Weierstrass  $\wp$ ,  $\wp'$  functions. Unfortunately, such a direct approach is not always satisfactory, especially if one desires an equation with good arithmetical properties.

A very basic example illustrates this phenomenon: let us consider the complex torus  $\mathbb{C}/\mathbb{Z}[i]$ . We may compute numerically the common Weierstrass coefficients and find

$$g_2(\mathbb{Z}[i]) = 189.07272012923385\dots, \quad g_3(\mathbb{Z}[i]) = 0.000000000\dots$$

While the second one seems to vanish clearly, the first one is difficult to recognize, since it turns to be the transcendental number  $\frac{\pi^2\Gamma(1/4)^4}{4\Gamma(3/4)^4}$ . On the other hand, it is well-known that the equation  $Y^2 = X^3 - X$  gives an algebraic model of this torus, with good reduction outside 2.

We will explain here a general method to find such nice equations for elliptic curves. The key ingredient will be the classical Jacobi theta functions. The models provided have very good arithmetical properties. For instance, they are not far from having good reduction everywhere.

---

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

*Key words*. Thetanullwerte, periods, elliptic curves, good reduction.

Partially supported by MCYT BFM2003-06768-C02-02.

In the last part of the paper, we will exhibit some families of elliptic curves with every good reduction; these families cover all the  $\overline{\mathbb{Q}}$ -isomorphism classes of elliptic curves.

The article contains an overview of previous results by the author on the application of theta functions to the determination of good equations and their periods for general hyperelliptic curves ([4], [5]). We have included them to help the reader to have a complete panorama of the ideas that lead to the particular method for elliptic curves. We have also included some recent unpublished results concerning elliptic curves with everywhere good reduction. Since they can be found in the papers cited in the bibliography, we have omitted most of the proofs.

Along the paper, we will use the word *algebraic* in a certain broad sense. For instance, when we say that a period of a curve is algebraic we mean that it comes from an algebraic differential form, i.e., a differential form defined over an algebraic extension of the definition field of the curve.

**1.1. Notation.** In the whole paper,  $\tau$  will always denote a complex number in the Poincaré upper half plane  $\mathbb{H}$ . A matrix in the Siegel upper half space  $\mathbb{H}_g$  will be written as  $Z$ . We will make use of the classical Jacobi Thetanullwerte:

$$\begin{aligned}\theta_2(\tau) &= \sum_{n \in \mathbb{Z}} q^{(n-1/2)^2/2}, \\ \theta_3(\tau) &= \sum_{n \in \mathbb{Z}} q^{n^2/2}, \quad (q = e^{2\pi i \tau}), \\ \theta_4(\tau) &= \sum_{n \in \mathbb{Z}} (-1)^n q^{n^2/2}\end{aligned}$$

as well as of the Riemann theta function, defined by:

$$\theta(z; Z) = \sum_{n \in \mathbb{Z}^g} \exp(\pi i n^t Z n + 2\pi i n^t z).$$

Finally, the ring of integers of a number field  $K$  will be written  $\mathcal{O}_K$ , and  $\overline{\mathbb{Z}}$  will denote the ring of integers of an algebraic closure  $\overline{\mathbb{Q}}$  of  $\mathbb{Q}$ .

## 2. Periods of algebraic differential forms on elliptic curves

Let us recall the classical uniformization of elliptic curves. Given  $\tau \in \mathbb{H}$ , the complex torus  $\mathbb{C}/\langle 1, \tau \rangle$  is mapped onto an elliptic curve  $E_\tau$

by the Weierstrass  $\wp(z)$  function and its derivative  $\wp'(z)$ .

$$\begin{aligned} \mathbb{C}/\langle 1, \tau \rangle &\xrightarrow{\varphi} E_\tau : Y^2 = 4X^3 - g_2(\tau)X - g_3(\tau) \\ z &\longrightarrow (\wp(z), \wp'(z)). \end{aligned}$$

The coefficients of the equation of  $E_\tau$  are given by the values of the Eisenstein series:

$$\begin{aligned} g_2(\tau) &= 60 \sum'_{m,n \in \mathbb{Z}} \frac{1}{(m+n\tau)^4}, \\ g_3(\tau) &= 140 \sum'_{m,n \in \mathbb{Z}} \frac{1}{(m+n\tau)^6}, \end{aligned}$$

of weight 4 and 6 respectively. A priori, we can say almost nothing about the algebraicity of the values of  $g_2(\tau)$ ,  $g_3(\tau)$ , even in the case that  $j(\tau) \in \overline{\mathbb{Q}}$ , that is, when  $E_\tau$  admits an algebraic model. In this situation, we will have in general that the canonical differential form will be not algebraic:

$$dz = \varphi^* \frac{dX}{Y} \notin H^0(E_\tau, \Omega^1_{\mathbb{C}(E_\tau)/\overline{\mathbb{Q}(j(\tau))}}).$$

The ultimate reason for this is that  $X, Y$  belong to  $\mathbb{C}(E_\tau)$ , but they are not defined over  $\overline{\mathbb{Q}(j(\tau))}$ , i.e., they are not built from an algebraic model for  $E_\tau$ . Let us try to build an algebraic differential form. We must begin with an algebraic model for  $E_\tau$ . We consider the Jacobi model:

$$E_k : Y^2 = (1 - X^2)(1 - k(\tau)^2 X^2),$$

given by the *modulus*  $k(\tau)$ . Since

$$j_E = 2^8 \frac{(k(\tau)^4 - k(\tau)^2 + 1)^3}{k(\tau)^4(k(\tau)^2 - 1)^2},$$

we have  $k(\tau) \in \overline{\mathbb{Q}(j(\tau))}$ , i.e., the Jacobi model is algebraic over  $\overline{\mathbb{Q}(j(\tau))}$ . The period lattice of this curve is  $\langle 4K(k), 4iK'(k) \rangle$ , where

$$\begin{aligned} K(k) &= \int_0^1 \frac{dx}{\sqrt{(1-x^2)(1-k^2x^2)}} = \frac{\pi}{2} \theta_3(\tau)^2, \\ K'(k) &= \int_1^{1/k} \frac{dx}{\sqrt{(x^2-1)(1-k^2x^2)}} = -i\tau K(k) \end{aligned}$$

are the complete elliptic integrals of the first kind. The uniformization of this curve is given by the Jacobi elliptic functions  $\text{sn}(u)$ ,  $\text{sn}'(u)$ , and

we have the following diagram:

$$\begin{array}{ccc}
 \mathbb{C}/\langle 1, \tau \rangle & \xrightarrow{\varphi} & Y^2 = 4X^3 - g_2(\tau)X - g_3(\tau) \\
 \downarrow *4K & & \downarrow \\
 \mathbb{C}/\langle 4K, 4iK' \rangle & \xrightarrow{\phi} & Y^2 = (1 - X^2)(1 - k(\tau)^2 X^2)
 \end{array}$$

$(z)$   $\xrightarrow{\varphi}$   $(\wp(z), \wp'(z))$   
 $(u)$   $\xrightarrow{\phi}$   $(\operatorname{sn} u, \operatorname{sn}' u)$

The functions  $X, Y$  giving the Jacobi model are now algebraic over  $\mathbb{Q}(j(\tau))$ , so that the differential form

$$du = \phi^* \frac{dX}{Y} \in H^0(E, \Omega^1_{E/\mathbb{Q}(j(\tau))})$$

is algebraic.

The classical Jacobi Thetanullwerte  $\theta_1(\tau), \theta_2(\tau), \theta_3(\tau)$  provide a general frame to study all the coefficients appearing in the diagram above from a common viewpoint. The starting point are the following equalities:

$$g_2(\tau) = \frac{2}{3}\pi^4(\theta_2(\tau)^8 + \theta_3(\tau)^8 + \theta_4(\tau)^8),$$

$$g_3(\tau) = \frac{4}{27}\pi^6(\theta_2(\tau)^4 + \theta_3(\tau)^4)(\theta_3(\tau)^4 + \theta_4(\tau)^4)(\theta_4(\tau)^4 - \theta_2(\tau)^4),$$

$$k(\tau) = \frac{\theta_2(\tau)^2}{\theta_3(\tau)^2},$$

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

$$K'(k) = -i\tau K(k),$$

$$du = 2\pi\theta_3(\tau)^2 dz.$$

If we take into account Jacobi's identity:

$$\theta_2(\tau)^4 + \theta_4(\tau)^4 = \theta_3(\tau)^4,$$

we conclude that the differential forms:

$$(1) \quad \begin{aligned} \omega_2 &= \pi\theta_3(\tau)\theta_4(\tau) dz, \\ \omega_3 &= \pi\theta_2(\tau)\theta_4(\tau) dz, \\ \omega_4 &= \pi\theta_2(\tau)\theta_3(\tau) dz, \end{aligned}$$

are also algebraic.

**Definition 1.** We call *theta-factors* of the periods of  $E_\tau$  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  $E_\tau$  are

$$\Lambda_{\tau,2} = \frac{1}{\sqrt{6}}\pi_2(\tau)\langle 1, \tau \rangle, \quad \Lambda_{\tau,3} = \frac{1}{\sqrt{6}}\pi_3(\tau)\langle 1, \tau \rangle, \quad \Lambda_{\tau,4} = \frac{1}{\sqrt{6}}\pi_4(\tau)\langle 1, \tau \rangle.$$

We now consider the Weierstrass coefficients corresponding to these period lattices:

**Definition 2.** Let  $\{i, j, k\} = \{2, 3, 4\}$ . The *modified Weierstrass coefficients* and the *modified discriminant* are

$$\begin{aligned} \mathcal{G}_{2,k}(\tau) &= g_2(\Lambda_{\tau,k}) \\ &= 6^2 \frac{g_2(\tau)}{\pi_k(\tau)^4} = 24 \left( \frac{\theta_2(\tau)^8 + \theta_3(\tau)^8 + \theta_4(\tau)^8}{\theta_i(\tau)^4 \theta_j(\tau)^4} \right), \\ \mathcal{G}_{3,k}(\tau) &= g_3(\Lambda_{\tau,k}) \\ &= 6^3 \frac{g_3(\tau)}{\pi_k(\tau)^6} \\ &= -32 \frac{(\theta_3(\tau)^4 + \theta_4(\tau)^4)(\theta_2(\tau)^4 - \theta_4(\tau)^4)(\theta_2(\tau)^4 + \theta_3(\tau)^4)}{\theta_i(\tau)^6 \theta_j(\tau)^6}, \\ \mathcal{D}_k(\tau) &= \Delta(\Lambda_{\tau,k}) \\ &= \frac{\Delta(\tau)}{\pi_k(\tau)^{12}} = \mathcal{G}_{2,k}(\tau)^3 - 27\mathcal{G}_{3,k}(\tau)^2 = 2^{10}3^6 \frac{\theta_k(\tau)^8}{\theta_i(\tau)^4 \theta_j(\tau)^4}. \end{aligned}$$

The interest of these new coefficients follows from:

**Theorem 3.** For  $k = 2, 3, 4$  the equation

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

is a model for  $E_\tau$  defined over  $\overline{\mathbb{Q}(j(\tau))}$ , whose discriminant is  $\mathcal{D}_k(\tau)$ .

The following relations can be easily checked:

**Proposition 4.** Let  $u(\tau) = \sqrt{(j(\tau) - 1728)}$ .

- a)  $\mathcal{G}_{2,k}(\tau)^3 - 9j(\tau)\mathcal{G}_{2,k}(\tau) - 432j(\tau) = 0$ ;
- b)  $\mathcal{G}_{3,k}(\tau)^6 - 48u(\tau)^2\mathcal{G}_{3,k}(\tau)^4 - u(\tau)^4(j - 2^8 3)\mathcal{G}_{3,k}(\tau)^2 - 2^{12}u(\tau)^6 = 0$ ;
- c)  $\mathcal{D}_k(\tau)^3 - 2^{10}3^7\mathcal{D}_k(\tau)^2 - 2^{12}3^{12}(j(\tau) - 768)\mathcal{D}_k(\tau) - 2^{30}3^{18} = 0$ .

We deduce:

**Theorem 5.** The modified Weierstrass coefficients  $\mathcal{G}_{2,k}(\tau)$ ,  $\mathcal{G}_{3,k}(\tau)$  and the modified discriminant  $\mathcal{D}_k(\tau)$  are algebraic integers over  $\mathbb{Z}[j(\tau)]$ .

In particular, the models introduced in Theorem 3 are not only algebraic, but integral models of  $E_\tau$ . In fact, they can be considered for any elliptic curve, not necessarily coming from a complex torus.

**Theorem 6.** Let  $E$  be an elliptic curve defined over  $K = \mathbb{Q}(j_E)$ . Let  $\mathcal{G}_2, \mathcal{G}_3, \mathcal{D} = \mathcal{G}_2^3 - 27\mathcal{G}_3^2$  be a solution of the equations in Proposition 4. Let  $\mathfrak{p}$  be a prime ideal in the integers ring  $\mathcal{O}_K$  of  $K$ , coprime with 6. If  $E$  has potentially good reduction at  $\mathfrak{p}$ , then

$$\mathcal{E} : Y^2 = 4X^3 - \mathcal{G}_2X - \mathcal{G}_3$$

has good reduction at the primes in  $L = K(\mathcal{G}_2, \mathcal{G}_3)$  over  $\mathfrak{p}$ .

A careful look at the relations in Proposition 4 shows that for generic  $\tau$  they are precisely the minimal equations of  $\mathcal{G}_2(\tau)$ ,  $\mathcal{G}_3(\tau)$ ,  $\mathcal{D}(\tau)$  over  $\mathbb{Q}(j(\tau))$ , since the polynomials on the left of the equalities are irreducible. But one also discovers that the element  $\mathfrak{D}(\tau) := \mathcal{D}(\tau)/(2^6 3^6)$  is also an algebraic integer over  $\mathbb{Z}[j(\tau)]$ . Unfortunately, we cannot divide  $\mathcal{G}_3(\tau)$  by 2 or 3, so that the equation appearing in Theorem 6 can not be improved so easily. Anyway, it would be desirable to build an equation with discriminant  $\mathfrak{D}(\tau)$ , since its reduction properties should be better. These equations will appear naturally when we study our problem for hyperelliptic curves in general.

### 3. Periods of algebraic differential forms on abelian varieties

The construction of algebraic differential forms on elliptic curves can be generalized to abelian varieties of any dimension. The recipe seems to be classical:

**Theorem 7** ([10], [9]). *Let  $A$  be a principally polarized abelian variety of dimension  $g$ , defined over a number field  $K$ , and let  $Z \in \mathbb{H}_g$  a normalized period matrix for  $A$  with respect to a fixed symplectic basis of  $H_0(A, \mathbb{Z})$ , so that  $A$  is analytically isomorphic to the complex torus  $T_Z := \mathbb{C}^g / (1_g \mid Z)$ .*

- a) *There exist  $g$  odd 2-torsion points  $w_1, \dots, w_g \in T_Z[2]^{\text{odd}}$  and one even 2-torsion point  $w_0 \in T_Z[2]^{\text{even}}$  such that*

$$\Omega_1(w_1, \dots, w_g; w_0; Z) := \frac{1}{\theta[w_0]} \begin{pmatrix} \frac{\partial \theta}{\partial z_1}(w_1, Z) & \dots & \frac{\partial \theta}{\partial z_g}(w_1, Z) \\ \vdots & \ddots & \vdots \\ \frac{\partial \theta}{\partial z_1}(w_g, Z) & \dots & \frac{\partial \theta}{\partial z_g}(w_g, Z) \end{pmatrix}$$

*is a non-singular matrix.*

- b) *The differential forms*

$$(\omega_1, \dots, \omega_g) = (dz_1, \dots, dz_g) \Omega_1(w_1, \dots, w_g; w_0; Z)$$

*yield a basis of  $H^0(A, \Omega_{\overline{K}}^1)$ , whose periods are*

$$\Omega_1(w_1, \dots, w_g; w_0; Z)(1_g \mid Z).$$

We remark that for  $g = 1$ , i.e., for elliptic curves, this theorem, combined with Jacobi's triple product identity, provides the differential forms  $\pi\theta_j(\tau)\theta_k(\tau)$ .

### 4. Periods of algebraic differential forms on hyperelliptic curves

The construction given in Theorem 7 depends on the choice of the 2-torsion points on the abelian variety. In the particular case that the abelian variety is the Jacobian variety  $J(C)$  of a hyperelliptic curve  $C$ , we have proposed to make this choice in a way that makes present the geometry of the curve (cf. [5]):

**Theorem 8.** *Let  $C/K$  be a hyperelliptic curve defined over a number field  $K$ , and let  $Z$  be a period matrix for  $C$ , so that  $J(C) \simeq \mathbb{C}^g/(1_g | Z)$ . We shall denote by  $\Pi: C \rightarrow J(C)$  the Abel-Jacobi map, normalized so that  $(\Pi(C^{(g-1)})) = \text{div}(\theta)$ .*

*Take any  $g$ -uple  $(W_1, \dots, W_g)$  of Weierstrass points on  $C$ , and let  $w_i := \Pi(\sum_{j \neq i} W_j) \in J(C)[2]^{\text{odd}}$ . Take any  $w_0 \in J(C)[2]^{\text{even}}$  such that  $\theta(w_0; Z) \neq 0$ . The differential forms*

$$(\tilde{\omega}_1, \dots, \tilde{\omega}_g) = \Pi^*((dz_1, \dots, dz_g)\Omega_1(w_1, \dots, w_g; w_0; Z))$$

*yield a basis of  $H^0(C, \Omega_{\overline{K}}^1)$  with periods*

$$\Omega_1(w_1, \dots, w_g; w_0; Z)(1_g | Z).$$

The geometric ideas behind this construction were applied in [3] to realize 2-dimensional factors of the jacobian of certain modular curves as the jacobian variety of genus 2 curves. They have also been applied in [2] to exhibit some examples of abelian surfaces with several polarizations.

## 5. Symmetric models for hyperelliptic curves

The explicit relation between the geometry of the hyperelliptic curve  $C$  and the differential forms on  $J(C)$  built in Theorem 8 allows the reconstruction of the curve from the period matrix. This is especially easy for genus 2 curves, since any basis of  $H^0(C, \Omega^1)$  has a very particular shape:

**Theorem 9.** *Let  $C/K$  be a genus 2 curve, and  $Z \in \mathbb{H}_2$  a normalized period matrix for  $C$ . Let  $\tilde{\omega}_1, \tilde{\omega}_2$  be the differential forms given by Theorem 8. There exist  $x, y \in \overline{K}(C)$  such that*

$$\text{a) } \tilde{\omega}_1 = \frac{dx}{y}, \tilde{\omega}_2 = x \frac{dx}{y}.$$

$$\text{b) } y^2 = x^5 + G_2x^4 + G_3x^3 + G_4x^2 + x, \text{ for certain } G_2, G_3, G_4 \in \overline{K}.$$

These equations turn to have nice arithmetical properties, so it is worth considering them for general hyperelliptic curves:

**Definition 10.** A symmetric model for a hyperelliptic curve  $C/K$  is an equation

$$C: Y^2 = X^{2g+1} + G_1X^{2g} + \dots + G_{2g-1}X^2 + X, \quad G_j \in \overline{K}.$$

We refer to [5] for the detailed presentation of symmetric models for hyperelliptic curves. We only mention here two of the main results about them:

**Theorem 11.** *Let  $C_{/K} : Y^2 = f(X)$  be a hyperelliptic curve defined over a number field  $K$ , with potentially good reduction at an odd prime  $\mathfrak{p} \in \text{Spec}(\mathcal{O}_K)$ . Given a symmetric model*

$$\mathcal{C} : Y^2 = X^{2g+1} + G_1 X^{2g} + \cdots + G_{2g-1} X^2 + X$$

for  $\mathcal{C}$  defined over  $L := K[G_1, \dots, G_{2g-1}]$ , and a prime  $\mathfrak{p}' \in \text{Spec}(\mathcal{O}_L)$ ,  $\mathfrak{p}' \mid \mathfrak{p}$ , we have:

- a) *The symmetric coefficients  $G_k$  are  $\mathfrak{p}'$ -integral.*
- b) *The symmetric model  $\mathcal{C}$  has good reduction at  $\mathfrak{p}'$ .*

A Jacobian Nullwert is the determinant of a Jacobian matrix of a set of  $g$  odd Riemann theta functions. The original interest of the Jacobian Nullwerte was its role in various generalizations of Jacobi's triple product identity, but they have revealed as a good tool for certain geometric constructions. One of these is given by the following theorem (cf. [5]):

**Theorem 12.** *The symmetric models for a complex hyperelliptic curve over  $\mathbb{C}$  can be explicitly computed from a normalized period matrix by means of Jacobian Nullwerte.*

The results in this section have been used in [1] to provide examples of genus 2 curves whose jacobian varieties are fake elliptic curves with complex multiplication.

## 6. Symmetric equations for elliptic curves

We now focus our attention in symmetric models for elliptic curves in general. We assume that we are working over a field  $K$  with  $\text{char}(K) \neq 2$ , and we consider the elliptic curve

$$E_G : Y^2 = X^3 + GX^2 + X, \quad G \in K.$$

The coefficient  $G$  appearing in a symmetric model for an elliptic curve and its corresponding discriminant will be called the *symmetric invariant* and the *symmetric discriminant* respectively. The values of the symmetric discriminant and the  $j$ -invariant of  $E_G$  are:

$$(2) \quad \mathfrak{D} = 16(G^2 - 4), \quad j = \frac{256(G^2 - 3)^3}{G^2 - 4} = \frac{(\mathfrak{D} + 16)^3}{\mathfrak{D}}.$$

Every class of  $\overline{K}$ -isomorphism of elliptic curves has six symmetric models, grouped in pairs, which share the same discriminant:

$$\begin{array}{c}
 G_{\pm 2} \rightsquigarrow \mathfrak{D}_2 \\
 \nearrow \\
 j \rightsquigarrow G_{\pm 3} \rightsquigarrow \mathfrak{D}_3 \\
 \searrow \\
 G_{\pm 4} \rightsquigarrow \mathfrak{D}_4
 \end{array}$$

The labeling of the different symmetric invariants introduced here follows from their interpretation as modular functions. As such, they can be expressed in terms of the Jacobi theta functions. We have:

$$G_{\pm 2}(\tau) := \pm \frac{\theta_3(\tau)^4 + \theta_4(\tau)^4}{\theta_3(\tau)^2 \theta_4(\tau)^2},$$

$$G_{\pm 3}(\tau) := \pm \frac{i(\theta_2(\tau)^4 - \theta_4(\tau)^4)}{\theta_2(\tau)^2 \theta_4(\tau)^2},$$

$$G_{\pm 4}(\tau) := \pm \frac{\theta_2(\tau)^4 + \theta_3(\tau)^4}{\theta_2(\tau)^2 \theta_3(\tau)^2}.$$

Concerning the symmetric discriminants, we find:

$$\mathfrak{D}_2(\tau) = \frac{16\theta_2(\tau)^8}{\theta_3(\tau)^4 \theta_4(\tau)^4},$$

$$\mathfrak{D}_3(\tau) = -\frac{16\theta_3(\tau)^8}{\theta_2(\tau)^4 \theta_4(\tau)^4},$$

$$\mathfrak{D}_4(\tau) = \frac{16\theta_4(\tau)^8}{\theta_2(\tau)^4 \theta_3(\tau)^4},$$

and these expressions show immediately that  $\mathfrak{D}_k(\tau) = \frac{1}{2^6 3^6} \mathcal{D}_k(\tau)$ , so that *symmetric models for elliptic curves are the models we were looking for* since the end of Section 2. In particular their arithmetical properties should be really nice, and this is the case:

**Proposition 13.** *Let  $A$  be a domain, with field of fractions  $K = \text{Fr}(A)$  of odd characteristic, and take  $G \in A$ .*

- a)  $E_G : Y^2 = X^3 + GX^2 + X$  is a stable curve over  $A[1/2]$ .
- b) The odd part of the conductor of  $E_G$  is  $N_{\text{odd}} = \prod_{\mathfrak{p}|G \pm 2} \mathfrak{p}$ .
- c)  $E_G$  has multiplicative reduction at the odd primes  $\mathfrak{p} \mid G \pm 2$ .

Reciprocally, we have:

**Theorem 14.** *Let  $E/A$  be an elliptic curve over a domain  $A$  as before. Let  $G$  a symmetric invariant for  $E$  and let  $L = \text{Fr}(A[G])$ .*

- a) If  $G$  is not  $\mathfrak{p}$ -integral at a prime  $\mathfrak{p} \in \text{Spec}(A[\frac{1}{2}][G])$ , then  $E$  has potentially multiplicative reduction at this prime.
- b) If  $j(E) \in A$  is integral, then  $E_G$  is an integral model for  $E$  over  $L$ , and it is minimal over  $A[\frac{1}{2}][G]$ .

We finish this presentation of symmetric models for elliptic curves observing that they carry an evident 2-torsion point, which gives raise to a 2-isogeny.

**Proposition 15.** *Let  $P = (0, 0) \in E_G[2](\mathbb{Q}(G))$ . The 2-isogenous elliptic curve  $E' := E_G/\langle P \rangle$  is:*

$$E' := Y^2 = X^3 + GX^2 - 4X - 4G.$$

A symmetric invariant and its corresponding symmetric discriminant for it are

$$G_{E'} = \frac{4G^2}{G^2 - 16}, \quad \mathfrak{D}_{E'} = \frac{2^{12}}{\mathfrak{D}}.$$

### 7. Symmetric discriminants as modular functions

The expression of the symmetric discriminants in terms of the Jacobi theta functions allows their study as modular functions.

**Proposition 16.** *Let  $S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ ,  $T = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ . Consider the level 2 congruence subgroups:  $\Gamma_0(2) = \langle S, TS^2T \rangle$ ,  $\Gamma_\theta = S^{-1}\Gamma^0(2)S$ ,  $\Gamma^0(2) = T\Gamma_0(2)T^{-1}$ .*

- a)  $\mathfrak{D}_2(\tau)$  is a Hauptmodul for the curve  $X_0(2) = \Gamma_0(2) \backslash \mathbb{H}^*$ .
- b)  $\mathfrak{D}_3(\tau)$  is a Hauptmodul for the curve  $X_\theta = \Gamma_\theta \backslash \mathbb{H}^*$ .
- c)  $\mathfrak{D}_4(\tau)$  is a Hauptmodul for the curve  $X^0(2) = \Gamma^0(2) \backslash \mathbb{H}^*$ .

Similarly, the symmetric invariants  $G_{\pm k}(\tau)$  turn to be *Hauptmoduln* for certain level 4 congruence groups.

The Fourier expansions of the symmetric discriminants are certainly nice:

$$\mathfrak{D}_2(\tau) = 2^{12}(q + 24q^2 + 300q^3 + 2624q^4 + 18126q^5 + O(q^6)),$$

$$\mathfrak{D}_3(\tau) = \frac{-1}{\sqrt{q}} - 24 - 276\sqrt{q} - 2048q - 11202q^{\frac{3}{2}} - 49152q^2 + O(q^3),$$

$$\mathfrak{D}_4(\tau) = \frac{1}{\sqrt{q}} - 24 + 276\sqrt{q} - 2048q + 11202q^{\frac{3}{2}} - 49152q^2 + O(q^3).$$

The interest of these expansions is reinforced when we compare their coefficients with the coefficients of the Fourier expansion of the  $j$ -invariant:

$$j(\tau) = 1/q + 744 + 196884q + 21493760q^2 + 864299970q^3 + O(q^5).$$

The small coefficients in the Fourier expansions of the symmetric discriminants indicate that these modular functions are well-suited for numerical computations (see [6] for a detailed discussion of this topic).

The relation between the  $j$ -invariant of an elliptic curve and its symmetric invariants implies the following functional equation:

$$\mathfrak{D}_r(\tau)^3 + 48\mathfrak{D}_r(\tau)^2 + (768 - j(\tau))\mathfrak{D}_r(\tau) + 2^{12} = 0,$$

which in turn generate the equalities:

$$\mathfrak{D}_2(\tau) + \mathfrak{D}_3(\tau) + \mathfrak{D}_4(\tau) = -48,$$

$$\mathfrak{D}_2(\tau)\mathfrak{D}_3(\tau)\mathfrak{D}_4(\tau) = -2^{12},$$

which are essentially Jacobi identities for the theta functions.

## 8. Elliptic curves with everywhere good reduction

We have seen in Section 6 that symmetric models have very good reduction properties. It is especially remarkable the fact that the locus of bad reduction of an elliptic curve given by a symmetric model coincides, up to even primes, with the locus of multiplicative reduction of the curve. In particular, when we have an elliptic curve with everywhere good reduction, symmetric models are near to be optimal, and hence constitute a good starting point to build a global minimal model.

We are going to consider this problem. Given an algebraic integer  $j \in \overline{\mathbb{Z}}$ , we want to find an elliptic curve  $E$  with this  $j$ -invariant and with everywhere good reduction. The relation between  $j$  and the symmetric discriminant:

$$j = \frac{(\mathfrak{D} + 16)^3}{\mathfrak{D}} \iff \mathfrak{D}^3 + 48\mathfrak{D}^2 + (768 - j)\mathfrak{D} + 2^{12} = 0$$

shows that they must be simultaneously integral:

$$j \in \overline{\mathbb{Z}} \iff \mathfrak{D} \in \overline{\mathbb{Z}}, \mathfrak{D} \mid 2^{12}.$$

If this is the case, we already know that the elliptic curve

$$E_G : Y^2 = X^3 + GX^2 + X, \quad G = \sqrt{\frac{\mathfrak{D} + 64}{16}}$$

has bad reduction only at primes in  $\mathbb{Q}(G)$  dividing 2. It is a natural temptation trying to arrange this equation at even primes to obtain a curve with everywhere good reduction. The immediate guess to do this is to apply Tate’s algorithm over the ring of integers  $\mathcal{O}_L$  of the field  $L = \mathbb{Q}(G)(E_G[3])$ . Unfortunately, this is not feasible in general, since the field  $L$  is very big, and generic computations cannot be performed on it.

We will try a less subtle approach: we will look directly for a Weierstrass substitution  $\left\{ \begin{matrix} x=u^2x'+r \\ y=u^3y'+u^2sx'+t \end{matrix} \right\}$  with  $u = \sqrt[12]{\mathfrak{D}}$  carrying to a new equation

$$Y^2 + a'_1XY + a'_3Y = X^3 + a'_2X^2 + a'_4X + a'_6$$

with  $a'_1, \dots, a'_6 \in \overline{\mathbb{Z}}$ . The integrality of the new coefficients is then translated into certain divisibility conditions. The results in the next subsections have been obtained in [7], where the proofs will appear.

### 8.1. Elliptic curves with unitary symmetric discriminant.

**Proposition 17.** *Let  $\mathfrak{D} \in \overline{\mathbb{Q}}$  be an algebraic unit. The Weierstrass equation*

$$\mathcal{E}_{/K} : Y^2 + \sqrt[4]{\mathfrak{D} + 64}XY = X^3 + X$$

*has everywhere good reduction over the ring of integers of the number field  $K = \mathbb{Q}(\sqrt[4]{\mathfrak{D} + 64})$ . Its discriminant and  $j$ -invariant are:*

$$\Delta_{\mathcal{E}} = \mathfrak{D}, \quad j_{\mathcal{E}} = \frac{(\mathfrak{D} + 16)^3}{\mathfrak{D}}.$$

This equation follows from the symmetric equation for  $\mathcal{E}$  given by  $\mathfrak{D}$ . It is a good moment to remember the 2-isogeny built at the end of Section 6: we can move it to this new model, to obtain a second equation with everywhere good reduction:

**Corollary 18.** *The Weierstrass equation*

$$\mathcal{E}'/K := \mathcal{E}/\langle(0,0)\rangle : Y^2 + \sqrt[4]{\mathfrak{D}+64}XY = X^3 - 4X - \sqrt{\mathfrak{D}+64}$$

has everywhere good reduction over the ring of integers of  $K$ . Its discriminant and  $j$ -invariant are:

$$\Delta_{\mathcal{E}'} = \mathfrak{D}^2, \quad j_{\mathcal{E}'} = \frac{(\mathfrak{D}+256)^3}{\mathfrak{D}^2}.$$

Let us see the easiest example: we take  $\mathfrak{D} = 1$  and find the elliptic curves:

$$\mathcal{E} : Y^2 + \sqrt[4]{65}XY = X^3 + X, \quad j_{\mathcal{E}} = 65^3,$$

$$\mathcal{E}' : Y^2 + \sqrt[4]{65}XY = X^3 - 4X - \sqrt{65}, \quad j_{\mathcal{E}'} = 257^3.$$

These two elliptic curves can be clearly defined over  $\mathbb{Q}$ , and they acquire everywhere good reduction over the quadratic fields  $\mathbb{Q}(\sqrt{\pm 65})$  (cf. [8]), but it is only over the quartic field  $\mathbb{Q}(\sqrt[4]{65})$  that they have a global minimal model with everywhere good reduction.

## 8.2. Elliptic curves with non-unitary symmetric discriminant and integral symmetric invariant.

**Proposition 19.** *Let  $\mathfrak{D} \in \overline{\mathbb{Z}}$  be an algebraic non-unitary integer, with  $\mathfrak{D} \mid 2^{12}$  in the ring of integers of  $K = \mathbb{Q}(\mathfrak{D})$ . Assume that  $G = \sqrt{\frac{\mathfrak{D}+64}{16}} \in \overline{\mathbb{Z}}$ . Let  $r$  be a root of the equation  $3r^4 + 4Gr^3 + 6r^2 - 1 = 0$  and let  $A = \sqrt{G+3r}$ ,  $B = \sqrt{r^3 + Gr^2 + r}$  with  $3r^2 + 2Gr + 1 = 2AB$ . The elliptic curve:*

$$\mathcal{E} : Y^2 + \frac{2A}{\sqrt[12]{\mathfrak{D}}}XY + \frac{2B}{\sqrt[4]{\mathfrak{D}}}Y = X^3$$

has everywhere good reduction over the ring of integers of the number field  $L = \mathbb{Q}(r, A, \sqrt[12]{\mathfrak{D}})$ . Its discriminant and  $j$ -invariant are:

$$\Delta_{\mathcal{E}} = 1, \quad j_{\mathcal{E}} = \frac{(\mathfrak{D}+16)^3}{\mathfrak{D}}.$$

As before, we can derive new families of elliptic curves with everywhere good reduction using the 2-isogeny between symmetric models. But now we have a second isogeny, since the curve  $\mathcal{E}$  has a rational 3-torsion point over  $L$ . We have

$$P = \left( -\frac{r}{\sqrt[6]{\mathfrak{D}}}, \frac{Ar-B}{\sqrt[4]{\mathfrak{D}}} \right) \in \mathcal{E}[2], \quad Q = (0,0) \in \mathcal{E}[3].$$

**Corollary 20.** *The elliptic curve*

$$\mathcal{E}'_{/K} := \mathcal{E}/\langle P \rangle : Y^2 + \frac{2A}{\sqrt[12]{\mathfrak{D}}}XY + \frac{2B}{\sqrt[4]{\mathfrak{D}}}Y = X^3 - \frac{5}{\sqrt[3]{\mathfrak{D}}}X - \frac{(4G + 5r)}{\sqrt{\mathfrak{D}}}$$

has everywhere good reduction over  $\mathbb{Q}(r, A, \sqrt[12]{\mathfrak{D}})$ .

**Corollary 21.** *The elliptic curve*

$$\mathcal{E}'_{/K} := \mathcal{E}/\langle (0, 0) \rangle : Y^2 + \frac{2A}{\sqrt[12]{\mathfrak{D}}}XY + \frac{2B}{\sqrt[4]{\mathfrak{D}}}Y = X^3 - \frac{20AB}{\sqrt[3]{\mathfrak{D}}} - \frac{4B(4A^3 + 7B)}{\sqrt{\mathfrak{D}}}$$

has everywhere good reduction over  $\mathbb{Q}(r, A, \sqrt[12]{\mathfrak{D}})$ .

**8.3. Elliptic curves with non-unitary symmetric discriminant and non integral symmetric invariant.**

**Proposition 22.** *Let  $\mathfrak{D} \in \overline{\mathbb{Z}}$  be an algebraic non-unitary integer, with  $\mathfrak{D} \mid 2^{12}$  in the ring of integers of  $K = \mathbb{Q}(\mathfrak{D})$ . Assume that  $G = \sqrt{\frac{\mathfrak{D}+64}{16}} \notin \overline{\mathbb{Z}}$ . Let  $r$  be a root of the equation  $3r^4 + 16Gr^3 + 96r^2 - 256 = 0$  and let  $A_1 = \sqrt{4G + 3r}$ ,  $B_1 = \sqrt{r^3 + 4Gr^2 + 16r} = (3r^2 + 8Gr + 16)/(2A_1)$ . The elliptic curve:*

$$\mathcal{E} : Y^2 + \frac{A_1}{\sqrt[12]{\mathfrak{D}}}XY + \frac{B_1}{4\sqrt[4]{\mathfrak{D}}}Y = X^3$$

has good reduction everywhere over  $\mathbb{Q}(r, A_1, \sqrt[12]{\mathfrak{D}})$ . Its discriminant and  $j$ -invariant are:

$$\Delta_{\mathcal{E}} = 1, \quad j_{\mathcal{E}} = \frac{(\mathfrak{D} + 16)^3}{\mathfrak{D}}.$$

Summing up, we have proven the following :

**Theorem 23.** *Every  $\overline{\mathbb{Q}}$ -isomorphism class of elliptic curves with everywhere potential good reduction admits one of the following models:*

$\mathfrak{D} \in \overline{\mathbb{Z}}^*$	$Y^2 + \sqrt[4]{\mathfrak{D} + 64}XY = X^3 + X$
$\mathfrak{D} \in \overline{\mathbb{Z}}, \mathfrak{D} \notin \overline{\mathbb{Z}}^*, G \in \overline{\mathbb{Z}}$	$Y^2 + \frac{2A}{\sqrt[12]{\mathfrak{D}}}XY + \frac{2B}{\sqrt[4]{\mathfrak{D}}}Y = X^3$
$\mathfrak{D} \in \overline{\mathbb{Z}}, \mathfrak{D} \notin \overline{\mathbb{Z}}^*, G \notin \overline{\mathbb{Z}}$	$\mathcal{E} : Y^2 + \frac{A_1}{\sqrt[12]{\mathfrak{D}}}XY + \frac{B_1}{4\sqrt[4]{\mathfrak{D}}}Y = X^3$

where  $\mathfrak{D}$  is a symmetric discriminant and  $A, B$ , and  $A_1, B_1$  are given by Propositions 19 and 22 respectively.

**References**

- [1] P. BAYER AND J. GUÀRDIA, On equations defining fake elliptic curves, *J. Théor. Nombres Bordeaux* **17(1)** (2005), 57–67.
- [2] J. GONZÁLEZ, J. GUÀRDIA AND V. ROTGER, Abelian surfaces of  $GL_2$ -type as Jacobians of curves, *Acta Arith.* **116(3)** (2005), 263–287.
- [3] E. GONZÁLEZ-JIMÉNEZ, J. GONZÁLEZ AND J. GUÀRDIA, Computations on modular Jacobian surfaces, in: “*Algorithmic number theory*” (Sydney, 2002), Lecture Notes in Comput. Sci. **2369**, Springer, Berlin, 2002, pp. 189–197.
- [4] J. GUÀRDIA, Jacobi Thetanullwerte, periods of elliptic curves and minimal equations, *Math. Res. Lett.* **11(1)** (2004), 115–123.
- [5] J. GUÀRDIA, Jacobian Nullwerte, periods and symmetric equations for hyperelliptic curves, *Ann. Inst. Fourier (Grenoble)*, to appear (2007).
- [6] J. GUÀRDIA, E. TORRES AND M. VELA, Stable models of elliptic curves, ring class fields, and complex multiplication, in: “*Algorithmic number theory*”, Lecture Notes in Comput. Sci. **3076**, Springer, Berlin, 2004, pp. 250–262.
- [7] J. GUÀRDIA AND M. VELA, Elliptic curves with everywhere good reduction, in preparation.
- [8] B. SETZER, Elliptic curves over complex quadratic fields, *Pacific J. Math.* **74(1)** (1978), 235–250.
- [9] G. SHIMURA, On the derivatives of theta functions and modular forms, *Duke Math. J.* **44(2)** (1977), 365–387.
- [10] A. WEIL, Sur les périodes des intégrales abéliennes, *Comm. Pure Appl. Math.* **29(6)** (1976), 813–819.

Departament de Matemàtica Aplicada IV  
Escola Politècnica Superior d'Enginyeria de Vilanova i la Geltrú  
Av. Víctor Balaguer s/n  
E-08800 Vilanova i la Geltrú (Barcelona)  
Spain  
E-mail address: guardia@mat.upc.edu