Convolution and square in abelian groups I

Yves Benoist

Abstract

We prove that the functional equation $f\star f(2\,t)=\lambda f(t)^2$, for t in $\mathbb{Z}/d\mathbb{Z}$ with d odd, admits a non-zero solution f if $\lambda=\sqrt{a}+i\sqrt{b}$ with a,b positive integers such that $a+b=d$ and $a\equiv\frac{(d+1)^2}{4}$ mod 4. The proof involves theta functions on elliptic curves with complex multiplication.

1 The functional equation

It is well known that elliptic curves, theta functions and modular forms are very useful tools both in Algebraic Geometry and in Number Theory -see [5]. In this paper, we focus on an elementary open problem raised by numerical experiments. The main surprise in this text is that the intriguing output of these numerical experiments cannot be understood without these tools.

1.1 Introduction

We will deal with a finite abelian group G of odd order d, which, most of the time, will be the cyclic group $G=\mathbb{Z}/d\mathbb{Z}$, and with the functional equation

$$f*f\,(2t)=\lambda\,f^2(t)\quad\text{for all } t \text{ in } G, \tag{1.1}$$

where the unknown is a non-zero function $f:G\to\mathbb{C}$ and where $\lambda\in\mathbb{C}$ is a parameter. This equation expresses a proportionality condition between the "convolution square" of f and its "multiplication square". A non-zero

2020 Math. subject class. Primary 11F03 ; Secondary 11F27

Key words Functional Equation, Convolution, Cyclic groups, Elliptic curves, Complex multiplication, Theta functions, Modular curve.

solution f of this functional equation (1.1) will be called a "λ-critical function on G" or, in short, a "λ-critical function", and a value λ for which such a function f exists will be called a "critical value on G", or a "d-critical value" when $G = \mathbb{Z}/d\mathbb{Z}$. Note that Equation (1.1) has been chosen so that it is invariant by translation on the variable t. This equation (1.1) can be rewritten as

$$\sum_{\ell \in G} f(k+\ell)\, f(k-\ell) = \lambda\, f(k)^2 \quad \text{for all } k \text{ in } G. \tag{1.2}$$

The aim of this text is to point out the interest of this functional equation by gathering unexpected results and questions based on numerical experiments and by relating this apparently naive functional equation to elliptic curves with complex multiplication.

Indeed, our main result, Theorem 2.3, gives explicit d-critical values. Eventhough the statement of this theorem is very short and purely elementary, surprisingly, our construction relies on the Jacobi theta functions $\theta(z, \tau)$ for special values of the parameter τ, and the key point in the proof relies on modularity properties due to Hecke (Lemma 3.8) of these theta functions.

I tried to keep this text as elementary and concrete as possible. In a second more technical paper [2], I will extend this construction of critical values to all finite abelian groups G by using the Riemann theta functions on higher dimensional abelian varieties, and their modularity properties as functions on the Siegel upper half-space – see Theorem 3.16.

I thank Gérard Laumon, Samuel Lelièvre and Emmanuel Ullmo for enlighting discussions on this project.

1.2 Comments

$\star$ Since d is odd, the value $\lambda = 0$ is not d-critical. Indeed the only function f for which $f * f = 0$ is $f = 0$.

$\star$ By analogy, one might look at Equation (1.1) on locally compact abelian groups G. When the group is $G = \mathbb{R}$ or $G = \mathbb{Z}$, the only L^2-solutions that I know are gaussian functions $f(t) = e^{at^2+bt+c}$ where $a, b, c \in \mathbb{C}$, $Re(a) < 0$, together with, when $G = \mathbb{Z}$, their restrictions to subgroups. When the group is $G = \mathbb{R}/\mathbb{Z}$, the only L^2-solutions that I know are constant functions.

1.3 Special critical values

In this section, we list a few d-critical values that are easy to find. We call them special.

$\star$ If we choose $f(0) = 1$ and $f(k) = \alpha$ to be constant for k in $G \smallsetminus \{0\}$, we find four critical values: we find $\lambda = 1$ when $\alpha = 0$, we find $\lambda = d$ when $\alpha = 1$, and we find $\lambda = \frac{d-3+\varepsilon\sqrt{D}}{2}$ when $\alpha = \frac{1-d-\varepsilon\sqrt{D}}{2(d-1)}$, with $\varepsilon = \pm 1$ and $D = (d-1)(d-9)$. Note that these d-critical values are real as soon as $d \geq 9$.

$\star$ If we choose f to be a gaussian function $f(k) := \eta^{-k^2}$ with $\eta := -e^{i\pi/d}$, we find the critical value $\lambda = \sqrt{d}$ when $d \equiv 1 \bmod 4$ and $\lambda = i\sqrt{d}$ when $d \equiv 3 \bmod 4$. Moreover, its opposite $-\lambda$ is also often a critical value. This is the case when d is not a square. But this is not always the case, for instance, when $d = 9$, the value -3 is not d-critical.

1.4 Induced critical values

In this section we explain how to construct d-critical values when d is a composite number starting from critical values for the factors of d. The method works for any abelian groups.

$\star$ Let $G_1 \subset G$ be finite abelian groups and λ_1 be a critical value on G_1 with λ_1-critical function f_1. Then λ_1 is also a critical value on G with λ-critical function $f := f_1 \mathbf{1}_{G_1}$.

$\star$ Let $G_1 \subset G$ be finite abelian groups, d_1 be the order of G_1 and λ_2 be a critical value on the quotient G/G_1 with λ_2-critical functions f_2. Then $\lambda := d_1\lambda_2$ is a critical value on G with λ-critical function $f := f_2 \circ \pi$ where $\pi : G \to G/G_1$ is the projection.

$\star$ Let $G = G_1 \times G_2$ be the product of two finite abelian groups, let λ_1 be a critical value on G_1 with λ_1-critical function f_1 and λ_2 be a critical value on G_2 with λ_2-critical function f_2. Then the product $\lambda := \lambda_1\lambda_2$ is a critical value on G with λ-critical function $f := f_1 \otimes f_2$.

The most interesting critical values will be those that are not special and that are not obtained by these "induction" methods.

1.5 Numerical experiments

The following lists of d-critical values rely on numerical experiments using the Buchberger's algorithm for computing Groebner basis (see [4, Chap. 2]).

We denote by b_d the size of the list.

For $3 \leq d \leq 9$ the complete lists of d-critical values are:

$\star$ $\boxed{d=3}$ $b_3 = 4$. $\lambda = 1,\ 3$, and $\pm i\sqrt{3}$.
$\star$ $\boxed{d=5}$ $b_5 = 6$. $\lambda = 1,\ 5,\ \pm\sqrt{5}$, and $1 \pm 2i$.
$\star$ $\boxed{d=7}$ $b_7 = 8$. $\lambda = 1,\ 7,\ \pm i\sqrt{7}$, and $\pm 2 \pm i\sqrt{3}$.
$\star$ $\boxed{d=9}$ $b_9 = 15$. $\lambda = 1,\ 9,\ 3,\ \pm i\sqrt{3},\ \pm 3i\sqrt{3},\ \pm 1 \pm 2i\sqrt{2}$, and $\pm\sqrt{5} \pm 2i$.

For $d = 11$ and 13, the lists below of d-critical values are still probably complete (After this paper was published, I checked in December 23 that the list for $d = 11$ is complete).

$\star$ $\boxed{d=11}$ $b_{11} = 20$. $\lambda = 1\ ,\ 11,\ 4 \pm \sqrt{5},\ \pm i\sqrt{11}$,
$2 \pm i\sqrt{7},\ \pm 2\sqrt{2} \pm i\sqrt{3}$, and $\pm(1+\varepsilon\sqrt{5}) \pm i\sqrt{5-2\varepsilon\sqrt{5}}$ with $\varepsilon = \pm 1$.

$\star$ $\boxed{d=13}$ $b_{13} = 18$. $\lambda = 1\ ,\ 13,\ 5 \pm 2\sqrt{3},\ \pm\sqrt{13}$,
$\pm 1 \pm 2i\sqrt{3},\ \pm\sqrt{5} \pm 2i\sqrt{2}$, and $\pm 3 \pm 2i$.

For $d = 15$ and 17, here are just a few d-critical values. These values were obtained by the guess and check method. Looking at the critical values for $d \leq 13$ one can guess a few critical values for $d = 15$ and 17. The key point of the method is that the Buchberger's algorithm is much faster when checking if a given λ is d-critical than when finding all the d-critical values (After this paper was published, I found in December 23 more values in both lists. They will be described in the third part of this series of papers.).

$\star$ $\boxed{d=15}$ $\lambda =$ product of a 3-critical and a 5-critical value, $\lambda = 6 \pm \sqrt{21}$,
$-3,\ -5,\ \pm(\sqrt{3} \pm i\sqrt{2})(\sqrt{2} \pm i)$,
$\pm 2 \pm i\sqrt{11},\ \pm 2\sqrt{2} \pm i\sqrt{7}$, and $1+\varepsilon\sqrt{5} \pm i\sqrt{9-2\varepsilon\sqrt{5}}$ with $\varepsilon = \pm 1$.

$\star$ $\boxed{d=17}$ $\lambda = 1\ ,\ 17,\ 7 \pm 4\sqrt{2},\ \pm\sqrt{17}$,
$\pm 1 \pm 4i,\ \pm\sqrt{5} \pm 2i\sqrt{3},\ 3 \pm 2i\sqrt{2},\ \pm\sqrt{13} \pm 2i$, and
$\pm(1 + 2\varepsilon\sqrt{2}) \pm 2i\sqrt{2 - \varepsilon\sqrt{2}}$ with $\varepsilon = \pm 1$.

For our numerical experiments we used SageMath and Maple softwares.

2 Critical values

One of the motivations of Proposition 2.1 and Theorem 2.3 below is to explain some of the intriguing patterns that occur in these experimental lists of critical values.

2.1 Properties of critical values

We first begin by a few properties of the critical values, that are valid on any finite abelian group.

Proposition 2.1. *Let G be a finite abelian group of odd order d, and λ a critical value on G, then:*
(i) all the Galois conjugates of λ are also critical values on G,
(ii) one has $|\lambda| \leq d$ with equality if and only if $\lambda = d$,
(iii) the ratio d/λ is also a critical value on G,
(iv) The ratio $\frac{\lambda-1}{2}$ is an algebraic integer.

Corollary 2.2. *There exist only finitely many critical values on G.*

Proof of Corollary 2.2. By Chevalley theorem on "the elimination of quantifiers in an algebraically closed field", the set of critical values for G is a constructible subset of $\mathbb{C}$. This means that either it is finite or has finite complement in $\mathbb{C}$. Since, by (ii), it is bounded it must be finite. □

Proof of Proposition 2.1. *(i)* Equations (1.2) have rational coefficients.

(ii) This follows from Cauchy-Schwarz inequality. Indeed, setting $\|f\|_\infty = \max_{k\in G} |f(k)|$ and $\|f\|_2 = (\sum_k |f(k)|^2)^{\frac{1}{2}}$, one has

$$|\lambda| \|f\|_\infty^2 = \|f \star f\|_\infty \leq \|f\|_2^2 \leq d \, \|f\|_\infty^2.$$

Hence $|\lambda| \leq d$. In case we have equality the function f must have constant modulus, and must satisfy $f(k+\ell)f(k-\ell) = f(k)^2$, for all k, ℓ. Hence f is proportional to a character and one has $\lambda = d$.

(iii) If f is a λ-critical function on G, then its Fourier transform $\widehat{f}$, which is given by, for every character $\chi : G \to \mathbb{C}^*$,

$$\widehat{f}(\chi) = \sum_{x\in G} f(x)\chi(x),$$

is a d/λ-critical function on the dual group $\widehat{G}$ which is isomorphic to G.

(iv) Let G_+ be a subset of G of cardinality $\frac{d-1}{2}$ such that for each non-zero $\ell \in G$ either ℓ or $-\ell$ is in G_+. The equations (1.2) can be rewritten as

$$\tfrac{\lambda-1}{2}\, f(k)^2 = \sum_{\ell \in G_+} f(k+\ell)\, f(k-\ell) \qquad \text{for all } k \text{ in } G \tag{2.1}$$

Let K be the subfield of $\mathbb{C}$ generated by the coefficients $f(k)$. To prove that $\lambda' := \frac{\lambda-1}{2}$ is an algebraic integer, it is enough to check that, for all non-archimedean absolute value $|.|_v$ on K, one has $|\lambda'|_v \leq 1$.
We set $\|f\|_v := \max_{\ell \in G} |f(\ell)|_v$, we choose k such that $\|f\|_v = |f(k)|_v$, and we compute

$$\begin{aligned} |\lambda'|_v \|f\|_v^2 = |\lambda' f(k)^2|_v &= |\sum_{\ell \in G_+} f(k+\ell) f(k-\ell)|_v \\ &\leq \max_{\ell \in G} |f(k+\ell)|_v |f(k-\ell)|_v \ \leq\ \|f\|_v^2. \end{aligned}$$

This proves that $|\lambda'|_v \leq 1$ as required. □

2.2 Construction of critical values

From now on, G will be the cyclic group $\mathbb{Z}/d\mathbb{Z}$. It is not clear from the definition that there does exist d-critical values that are non-induced and non-special. The following theorem tells us that this is always the case for $d \geq 5$.

Theorem 2.3. *Let a,b be positive integers with $a+b=d$ and $a \equiv \frac{(d+1)^2}{4} \bmod 4$. Then the complex number $\lambda := \sqrt{a} + i\sqrt{b}$ is a d-critical value.*

Remark 2.4. The congruence assumption in Theorem 2.3 is equivalent to

$$a - b \equiv 1 \bmod 4 \quad \text{and} \quad ab \equiv 0 \bmod 4. \tag{2.2}$$

A more concrete way to state Theorem 2.3 is:

For $d \equiv 1 \bmod 4$, the following values are d-critical:
$\sqrt{d}$, $\sqrt{d-4}+2i$, $\sqrt{d-8}+2i\sqrt{2}$, $\sqrt{d-12}+2i\sqrt{3}$, ...

For $d \equiv 3 \bmod 4$, the following values are d-critical:
$i\sqrt{d}$, $2+i\sqrt{d-4}$, $2\sqrt{2}+i\sqrt{d-8}$, $2\sqrt{3}+i\sqrt{d-12}$, ...

More precisely, we will see that, surprisingly, for these values λ, the set of λ-critical functions has positive dimension. Indeed, we will construct a one-parameter family of λ-critical functions using a suitable Jacobi theta function.

Before that we discuss the above congruence condition on a.

Lemma 2.5. *Let a,b be positive integers with $a+b=d$ and let $\lambda := \sqrt{a}+i\sqrt{b}$. The number $\frac{\lambda-1}{2}$ is an algebraic integer if and only if $a \equiv \frac{(d+1)^2}{4} \bmod 4$.*

In particular, by Proposition 2.1.*iv*, when $a \not\equiv \frac{(d+1)^2}{4} \bmod 4$, the complex number $\lambda = \sqrt{a} + i\sqrt{b}$ can not be a d-critical value.

Remark 2.6. Note that, for any algebraic number λ, one has the equivalence:

$$\nu := \tfrac{\lambda-1}{2} \text{ is an algebraic integer } \iff \nu' := \tfrac{\lambda^2-1}{4} \text{ is an algebraic integer.} \quad (2.3)$$

Indeed, theses two elements ν and ν' are related by the equation $\nu^2 + \nu = \nu'$.

Proof of Lemma 2.5. The number $\nu' := \frac{\lambda^2-1}{4}$ is equal to $\nu' = \frac{a-b-1}{4} + i\frac{\sqrt{ab}}{2}$. It is an algebraic integer if and only if $a - b \equiv 1 \bmod 4$ and $ab \equiv 0 \bmod 4$. As seen in (2.2), this condition is equivalent to $a \equiv \frac{(d+1)^2}{4} \bmod 4$. □

Corollary 2.7. *Let p,q be positive integers with p odd and q even and let $d := p^2 + q^2$. Then the complex number $\lambda := p + iq$ is a d-critical value.*

Proof. Condition (2.2) is true: $p^2 - q^2 \equiv 1 \bmod 4$ and $p^2q^2 \equiv 0 \bmod 4$. □

2.3 More numerical experiments

A reasonable aim in this topic would be to give, for each d the list of the d-critical values λ, and for each λ the description of the projective algebraic variety given by the λ-critical functions (number of connected components, their dimension,...).

Here are a few less ambitious questions supported by numerical experiments that suggest that some hidden structure has to be understood.

The first question deals with the properties of the λ-critical functions when λ belongs to a real or imaginary quadratic number field.

Question 2.8. *Let d be an odd integer and λ a d-critical value which is quadratic. Does there exist an even λ-critical function?*

That is a λ-critical function f such that $f(-k) = f(k)$ for all k.

We checked, using numerical experiments, that this is true for $d \leq 11$. Unfortunately this is not true when λ is not quadratic as $2\sqrt{2}-1+2i\sqrt{2+\sqrt{2}}$.

The second question deals with the properties of the d-critical values.

Question 2.9. *Let d be an odd prime and λ a d-critical value. Are λ and d/λ Galois conjugate, except for $\lambda = 1$ and $\lambda = d$?*

In all our numerical examples the non-real critical values λ have a Galois conjugate in $\mathbb{C}$ with absolute value equal to $\sqrt{d}$.

On the other hand, using numerical experiments, we found an example of non real d-critical value λ whose absolute value is not equal to $\sqrt{d}$. In this example, one has $d = 43$.

The third question deals with critical values that are real quadratic.

Question 2.10. *Let d be an odd prime and λ a d-critical value which is a real quadratic number. Is such a λ special?*

We recall that special means that $\lambda = 1$, d, $\pm\sqrt{d}$, or $\frac{d-3\pm\sqrt{(d-1)(d-9)}}{2}$.

Note that the d-critical values which are quadratic over $\mathbb{Q}$ and non-real can be described up to sign thanks to Proposition 2.1 and Theorem 2.3.

We checked, using numerical experiments, that this is true for $d \leq 11$.

The last question deals with critical values that are quadratic over $\mathbb{Q}$ but are non real. More precisely it deals with the sign of $Re(\lambda)$ in Theorem 2.3.

Question 2.11. *Let d be an odd integer and a,b be positive integers with $a \equiv \frac{(d+1)^2}{4} \bmod 4$ and $a+b=d$. If $d \not\equiv 2 \bmod 3$, is the number $\lambda := -\sqrt{a}+i\sqrt{b}$ a d-critical value?*

Moreover, for each $d \equiv 2 \bmod 3$, one still expects the answer to this question to be true with at most one exception. Recall that the interesting case is when the critical value λ is quadratic over $\mathbb{Q}$ i.e. when the integer a is a square (see Remark 3.9).

We checked, using numerical experiments, that $-1+2i$ and $-2+i\sqrt{7}$ are not critical values and that, for $d \leq 23$, the only other possible exceptions are $-3+2i\sqrt{2}$ and $-4+i\sqrt{7}$.

There is another similar question in the case where $b = 0$: let $d = a_0^2$ be the square of an odd integer $a_0 \geq 3$. We know that this integer a_0 is a d-critical value. But when is its opposite $-a_0$ also d-critical? I checked, using numerical experiments, that -3 is not 9-critical but that -5 is 25-critical.

3 Theta functions and elliptic curves

Our aim now is to prove Theorem 2.3.

3.1 Main result

We recall the definition of the Jacobi theta function:

$$\theta_\tau(z) = \theta(z,\tau) := \sum_{m\in\mathbb{Z}} e^{i\pi\tau m^2} e^{2i\pi m z}, \text{ for } z \in \mathbb{C} \text{ and } \tau \in \mathbb{H},$$

where $\mathbb{H}$ is the upper half plane $\mathbb{H} = \{\tau \in \mathbb{C} \mid Im(\tau) > 0\}$. This function is 1-periodic: $\theta_\tau(z+1) = \theta_\tau(z)$. We can now explain our construction of λ-critical functions on $\mathbb{Z}/d\mathbb{Z}$.

Definition 3.1. We will say that the function θ_τ is (λ, d)-critical if, for all z in $\mathbb{C}$, the function $f_{z,\tau} : \ell \mapsto \theta(z+\ell/d, \tau)$ is λ-critical on $\mathbb{Z}/d\mathbb{Z}$.

This means that, for all z in $\mathbb{C}$,

$$\sum_{\ell\in\mathbb{Z}/d\mathbb{Z}} \theta(z+\ell/d,\tau)\,\theta(z-\ell/d,\tau) \;=\; \lambda\,\theta(z,\tau)^2.$$

Theorem 2.3 is a special case of the following Proposition 3.2.(a). The whole Proposition 3.2 tells us more. It tells us exactly for which parameters d, λ, τ, the function θ_τ is (λ, d)-critical.

Proposition 3.2. *Let a,b be positive integers with* $a \equiv \frac{(d+1)^2}{4} \bmod 4$ *and* $a+b=d$. *Set* $\lambda_0 := \sqrt{a} + i\sqrt{b}$ *and*

$$\tau_0 \;:=\; \tfrac{1}{4d^2}(a - b - d^2 + 2i\sqrt{ab}). \tag{3.1}$$

(a) *The function* θ_{τ_0} *is* (λ_0, d)*-critical.*
(b) *Conversely, let* $\tau \in \mathbb{H}$ *such that the function* θ_τ *is* (λ, d)*-critical, then one has* $\lambda = \pm\sqrt{a} \pm i\sqrt{b}$ *with a, b as above.*
(c) *The function* θ_τ *is* (λ, d)*-critical for* $\lambda = \pm\lambda_0$ *if and only if* $\tau = (k+\tau_0)/p$ *with* τ_0 *as above,* $k \in \mathbb{Z}$ *and* $p > 0$ *a divisor of the integer* $N_k := d^2\,|k+\tau_0|^2$.
(d) *The above sign* $\varepsilon = \pm$ *is given by the Jacobi symbol* $\varepsilon = (\frac{p}{4k-1})$.

Remember that the Jacobi symbol $(\frac{\gamma_0}{\delta_0}) = \pm 1$ is defined for two relatively prime integers γ_0 and δ_0 with δ_0 odd, and that, by convention, when δ_0 is negative, it is given by $(\frac{\gamma_0}{\delta_0}) = (\frac{\gamma_0}{-\delta_0})$.

Note also that, in view of Point (b), the assumption $\lambda = \pm\lambda_0$ in Point (c) is not restrictive since one has the equivalence:

$$\theta_\tau \text{ is } (\lambda, d)\text{-critical} \iff \theta_{-\overline{\tau}} \text{ is } (\overline{\lambda}, d)\text{-critical.}$$

Remark 3.3. The parameter τ_0 will be called the *fundamental parameter* and the parameters $\tau_{k,p} := (k + \tau_0)/p$ the *associated parameters*. These parameters $\tau_{k,p}$ and the integers N_k can also be given by the simple formulas with $m_0 := \frac{a-b-d^2}{4}$ and $N_0 := \frac{(d+1)^2-4a}{16}$:

$$\boxed{\tau_{k,p} = \tfrac{1}{d^2 p}(d^2 k + m_0 + i\sqrt{ab/4})} \text{ where } \boxed{p \,|\, N_k := d^2k^2 + 2m_0 k + N_0}.$$

Example 3.4. *To be very concrete, we give below the list of all values $\tau = \tau_{k,p}$ for which θ_τ is $(\pm\lambda_0, d)$-critical with k in $\mathbb{Z}$ and p divisor of N_k, when $d \leq 9$.*

$\star$ $d = 5$, $\lambda_0 = 1 + 2i$: $\tau_{k,p} = \frac{1}{25p}(25k - 7 + i)$ *where* $p \,|\, 25k^2 - 14k + 2$.
$\star$ $d = 7$, $\lambda_0 = 2 + i\sqrt{3}$: $\tau_{k,p} = \frac{1}{49p}(49k - 12 + i\sqrt{3})$ *where* $p \,|\, 49k^2 - 24k + 3$.
$\star$ $d = 9$, $\lambda_0 = 1 + 2i\sqrt{2}$: $\tau_{k,p} = \frac{1}{81p}(81k - 22 + i\sqrt{2})$ *where* $p \,|\, 81k^2 - 44k + 6$.
$\star$ $d = 9$, $\lambda_0 = \sqrt{5} + 2i$: $\tau_{k,p} = \frac{1}{81p}(81k - 20 + i\sqrt{5})$ *where* $p \,|\, 81k^2 - 40k + 5$.

Given d and λ_0, we have seen that it is always possible to choose k and p such that $\lambda = \varepsilon\lambda_0$ with sign $\varepsilon = (\frac{p}{4k-1})$ equal to $+1$: we just choose $p = 1$.

On the other hand, given d and λ_0, it is sometimes possible to choose k and p such that $\lambda = \varepsilon\lambda_0$ with sign $\varepsilon = (\frac{p}{4k-1})$ equal to -1. For instance,
$\star$ when $\lambda = -2 - i\sqrt{3}$ with $\tau = \frac{1}{98}(37 + i\sqrt{3})$, or
$\star$ when $\lambda = -\sqrt{5} - 2i$ with $\tau = \frac{1}{162}(61 + i\sqrt{5})$.
We mention the following corollary that tells us exactly when this is possible.

Corollary 3.5. *Let a,b be positive integers with $a \equiv \frac{(d+1)^2}{4} \bmod 4$ and $a+b=d$. Set $\lambda := -\sqrt{a} - i\sqrt{b}$. There exists τ in $\mathbb{H}$ whose function θ_τ is (λ, d)-critical if and only if either a is not a square in $\mathbb{Z}$ or $-b$ is not a square in $\mathbb{Z}/2a\mathbb{Z}$.*

Concretely, here are a few special cases of our criteria for such a function θ_τ to exist, in which a is a square in $\mathbb{Z}$ and b is either 4ℓ or $4\ell - 1$ with ℓ a positive integer:

$\star$ When $\lambda = -1 - 2i\sqrt{\ell}$: never.
$\star$ When $\lambda = -3 - 2i\sqrt{\ell}$: $\ell \equiv 1 \bmod 3$.
$\star$ When $\lambda = -5 - 2i\sqrt{\ell}$: $\ell \equiv 2$ or $3 \bmod 5$.
$\star$ When $\lambda = -2 - i\sqrt{4\ell - 1}$: $\ell \equiv 1 \bmod 2$.
$\star$ When $\lambda = -4 - i\sqrt{4\ell - 1}$: $\ell \equiv 1 \bmod 2$.
$\star$ When $\lambda = -6 - i\sqrt{4\ell - 1}$: $\ell \equiv 1, 2, 3$ or $5 \bmod 6$.

The proof of this corollary that relies on quadratic reciprocity is left to the reader. We will not use it below. The rest of the paper is devoted to the proof of Proposition 3.2.

3.2 Preliminary formulas

The proof of Proposition 3.2.(a) relies on three classical formulas for the theta functions, the "addition formula", the "isogeny formula", the "transformation formula". We will only need special cases of these formulas that we state below.

We need to introduce the theta functions[1]

$$\begin{aligned} \theta_{[0]}(z) = \theta_{[0]}(z,\tau) &:= \sum_{m \text{ even}} e^{i\pi\frac{\tau}{2}m^2} e^{2i\pi mz} \\ \theta_{[1]}(z) = \theta_{[1]}(z,\tau) &:= \sum_{m \text{ odd}} e^{i\pi\frac{\tau}{2}m^2} e^{2i\pi mz}. \end{aligned}$$

Note that one has the equalities:

$$\theta_{[0]}(z,\tau) = \theta(2z, 2\tau) \quad \text{and} \quad \theta_{[0]}(z,\tau) + \theta_{[1]}(z,\tau) = \theta(z, \tau/2). \tag{3.2}$$

Here is the first formula that we need.

Lemma 3.6. Addition formula *For all z, w in $\mathbb{C}$, $\tau \in \mathbb{H}$, one has*

$$\theta(z+w,\tau)\theta(z-w,\tau) = \theta_{[0]}(w,\tau)\theta_{[0]}(z,\tau) + \theta_{[1]}(w,\tau)\theta_{[1]}(z,\tau). \tag{3.3}$$

Proof. Just write the left-hand side as a double sum over m, n in $\mathbb{Z}$ and split this double sum according to the parity of $m-n$. □

Here is the second formula which is simple but useful.

[1] With other "classical" notations for theta functions as in [3], one has the equalities, $\theta_{[0]}(z,\tau) = \theta_{0,0}(2z,2\tau) = \theta\begin{bmatrix}0\\0\end{bmatrix}(2z,2\tau)$ and $\theta_{[1]}(z,\tau) = \theta_{1,0}(2z,2\tau) = \theta\begin{bmatrix}1/2\\0\end{bmatrix}(2z,2\tau)$.

Lemma 3.7. Isogeny formula *For $\tau \in \mathbb{H}$, d odd positive integer, one has*

$$\sum_{\ell \in \mathbb{Z}/d\mathbb{Z}} \theta_{[0]}(\ell/d, \tau) = d\,\theta_{[0]}(0, d^2\tau) \quad \text{and} \quad \sum_{\ell \in \mathbb{Z}/d\mathbb{Z}} \theta_{[1]}(\ell/d, \tau) = d\,\theta_{[1]}(0, d^2\tau).$$

Proof. Just write the left-hand sides as a double sum over m in $\mathbb{Z}$ and ℓ in $\mathbb{Z}/d\mathbb{Z}$ and notice that $\sum_{\ell \in \mathbb{Z}/d\mathbb{Z}} e^{2i\pi\ell m/d}$ is equal to d when d divides m and is equal to 0 otherwise. □

The last formula deals with an element $\sigma = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{SL}(2, \mathbb{Z})$.

Lemma 3.8. Transformation formula *If $\sigma \equiv \mathbb{1} \bmod 2$, and $\gamma > 0$, then*

$$\theta(0, \sigma\tau) \;=\; i^{\frac{\delta-1}{2}} \left(\tfrac{\gamma}{\delta}\right) (\gamma\tau + \delta)^{\frac{1}{2}}\, \theta(0, \tau). \tag{3.4}$$

In this formula, the $\mathrm{SL}(2, \mathbb{Z})$ action on the upper half plane $\mathbb{H}$ is the standard action $\sigma\tau = \frac{\alpha\tau+\beta}{\gamma\tau+\delta}$, the number $z^{\frac{1}{2}}$ is the square root of a complex number $z \in \mathbb{H}$ whose real part is non negative, and the symbol $\left(\frac{\gamma}{\delta}\right) = \pm 1$ is still the Jacobi symbol.

Note that Formula (3.4) can be equivalently rewritten as

$$\theta(0, \sigma\tau) \;=\; \varepsilon_\delta \left(\tfrac{2\gamma}{\delta}\right) (\gamma\tau + \delta)^{\frac{1}{2}}\, \theta(0, \tau),$$

where $\varepsilon_\delta = 1$ when $\delta \equiv 1 \bmod 4$, and $\varepsilon_\delta = -i$ when $\delta \equiv 3 \bmod 4$.

Proof. Up to sign, Formula (3.4) follows from the following two formulas

$$\begin{aligned} \theta(0, \tau + 2) &= \theta(0, \tau), \\ \theta(0, -1/\tau) &= (-i\tau)^{\frac{1}{2}}\, \theta(0, \tau). \end{aligned}$$

and from the fact that the map $(\sigma, \tau) \mapsto \sigma\tau + \delta$ is a cocycle on $\mathrm{SL}(2, \mathbb{Z}) \times \mathbb{H}$. The precise determination of the sign is a classical issue due to Hecke. It can be found for instance in [8, p.181] in [6, p.148] or in [7, p.32]. □

Remark 3.9. This precise determination of the sign is important for us because it will allow us to decide whether the critical value we will find is $\lambda = \sqrt{a} + i\sqrt{b}$ or its opposite. This is particularly important when a is a square, because in this case λ and $-\lambda$ are not Galois conjugate and one can not apply Proposition 2.1.i.

The following corollary of Lemma 3.8 will be very useful.

Corollary 3.10. *If $\sigma \equiv \pm \mathbb{1} \bmod 4$, then, for all τ in $\mathbb{H}$, one has*

$$\frac{\theta_{[0]}(0,\sigma\tau)}{\theta_{[0]}(0,\tau)} \;=\; \frac{\theta_{[1]}(0,\sigma\tau)}{\theta_{[1]}(0,\tau)}\,. \tag{3.5}$$

Proof. Let

$$\sigma' = \begin{pmatrix} \alpha & \beta' \\ \gamma' & \delta \end{pmatrix} \text{ and } \sigma'' = \begin{pmatrix} \alpha & \beta'' \\ \gamma'' & \delta \end{pmatrix},$$

with $\beta' = 2\beta$, $\gamma' = \gamma/2$ and $\beta'' = \beta/2$, $\gamma'' = 2\gamma$, so that

$$\sigma'(2\tau) = 2\sigma\tau \;\text{ and }\; \sigma''(\tau/2) = \tfrac{1}{2}\sigma\tau\,.$$

Since the matrix σ is equal to $\pm\mathbb{1} \bmod 4$, the two matrices σ' and σ'' are equal to $\mathbb{1} \bmod 2$. Therefore we can apply the transformation formula in Lemma 3.8 to both pairs $(\sigma', 2\tau)$ and $(\sigma'', \tau/2)$. Using the multiplicativity properties of the Jacobi symbol, we see that the following two ratios are given by the same formula

$$\frac{\theta(0,2\sigma\tau)}{\theta(0,2\tau)} = \frac{\theta(0,\frac{1}{2}\sigma\tau)}{\theta(0,\frac{1}{2}\tau)}.$$

We now conclude thanks to Equalities (3.2). □

3.3 The condition on theta contants

The first step in the proof of Proposition 3.2 is the following criterion on λ, τ which ensures that the functions $f_{z,\tau}$ are λ-critical. This criterion is a relation between "theta constants", i.e. theta functions evaluated at $z = 0$.

Lemma 3.11. *Let $\tau \in \mathbb{H}$ and $\lambda \in \mathbb{C}$. The function θ_τ is (λ, d)-critical if and only if one has the equalities*

$$\lambda = d\,\frac{\theta_{[0]}(0,d^2\tau)}{\theta_{[0]}(0,\tau)} = d\,\frac{\theta_{[1]}(0,d^2\tau)}{\theta_{[1]}(0,\tau)}\,. \tag{$T_{\lambda,\tau}$}$$

Proof. For w in $\mathbb{C}$ we introduce the function

$$z \mapsto F_w(z) = F_w(z,\tau) := \theta(z+w,\tau)\,\theta(z-w,\tau).$$

We want to know when the two functions $\sum_\ell F_{\ell/d}$ and $F_0 = \theta^2$ are proportional. The key point of the proof is that all these functions F_w live in the

same two-dimensional vector space and that this vector space has a very convenient basis: $(\theta_{[0]}, \theta_{[1]})$. We only have to express that the coefficients of our two functions in this basis are proportional. These coefficients are given by the following calculation in which we apply successively the addition formula and the isogeny formula,

$$\begin{aligned}\sum_{\ell} F_{\ell/d}(z,\tau) &= \sum_{\ell} \theta_{[0]}(\ell/d,\tau)\,\theta_{[0]}(z,\tau) + \sum_{\ell} \theta_{[1]}(\ell/d,\tau)\,\theta_{[1]}(z,\tau) \\ &= d\,\theta_{[0]}(0,d^2\tau)\,\theta_{[0]}(z,\tau) + d\,\theta_{[1]}(0,d^2\tau)\,\theta_{[1]}(z,\tau) \quad \text{and}\end{aligned}$$

$$\theta(z,\tau)^2 = \theta_{[0]}(0,\tau)\,\theta_{[0]}(z,\tau) + \theta_{[1]}(0,\tau)\,\theta_{[1]}(z,\tau).$$

These two functions are proportional with proportionality factor λ if and only if one has

$$\lambda = d\,\frac{\theta_{[0]}(0,d^2\tau)}{\theta_{[0]}(0,\tau)} = d\,\frac{\theta_{[1]}(0,d^2\tau)}{\theta_{[1]}(0,\tau)}\ .$$

This is the criterion $(T_{\lambda,\tau})$. □

3.4 The modular curve $X(4)$

In order to interpret the condition $(T_{\lambda,\tau})$, the following classical description of the modular curve $X(4)$ will be very useful.

For $m \geq 1$, we introduce the principal congruence subgroup of level m

$$\Gamma(m) := \{\sigma \in \mathrm{SL}(2,\mathbb{Z}) \mid \sigma \equiv \pm\mathbb{1} \mod m\}$$

and the modular curve of level m

$$X(m) := \Gamma(m)\backslash\mathbb{H}.$$

Note that the element $-\mathbb{1} \in \mathrm{SL}(2,\mathbb{Z})$ acts trivially on $\mathbb{H}$. It is classical that $X(m)$ is a Riemann surface with finitely many cusps whose genus can be calculated thanks to Hurwitz formula. In this elementary paper we will only deal with $m = 4$. In this case, $X(4)$ has genus zero and six cusps. The following lemma gives a nice interpretation of this fact.

We introduce the meromorphic function Φ on $\mathbb{H}$ given by, for all τ in $\mathbb{H}$,

$$\Phi(\tau) := \frac{\theta_{[1]}(0,\tau)}{\theta_{[0]}(0,\tau)}.$$

Lemma 3.12. *The map Φ induces a biholomorphism*

$$\varphi : X(4) \longrightarrow \mathbb{P}^1\mathbb{C} \smallsetminus \{0, \infty, \pm 1, \pm i\}.$$

This lemma tells us that, as an hyperbolic surface, $X(4)$ is the "regular ideal octahedron".

The statement of this lemma is equivalent to the following four facts on the meromorphic map Φ.
(a) For all σ in $\Gamma(4)$ and all τ in $\mathbb{H}$ one has $\Phi(\sigma\tau) = \Phi(\tau)$.
(b) For all τ in $\mathbb{H}$, one has $\Phi(\tau) \neq 0, \infty, \pm 1, \pm i$.
(c) If $\Phi(\tau) = \Phi(\tau')$, there exists σ in $\Gamma(4)$ such that $\tau' = \sigma\tau$.
(d) For all $z \neq 0, \infty, \pm 1, \pm i$, there exists τ in $\mathbb{H}$ with $\Phi(\tau) = z$.

Note that the first fact (a) is the most important one for us in order to prove Theorem 2.3 and that it is just a restatement of Corollary 3.10.

Proof of Lemma 3.12. This lemma is classical for the experts. We will just relate it to the existing litterature. We will deduce these four facts from a very similar statement in Mumford's book [7]. In this book, Mumford uses the four Jacobi theta-functions $\theta_{a,b}$ with a, b equal to 0 or 1, given by

$$\theta_{a,b}(z,\tau) = \sum_{m\in\mathbb{Z}} e^{i\pi\tau(m+\frac{a}{2})^2} e^{2i\pi(m+\frac{a}{2})(z+\frac{b}{2})}$$

It is proven in [7, Theorem 10.1 p.51] that the map Ψ given in homogeneous coordinates by

$$\Psi : \tau \mapsto [\theta_{0,0}^2(0,\tau), \theta_{0,1}^2(0,\tau), \theta_{1,0}^2(0,\tau)]$$

induces an biholomophism ψ between the curve $X(4)$ and the curve

$$C := \{[x_0, x_1, x_2] \in \mathbb{P}^2\mathbb{C} \mid x_0^2 = x_1^2 + x_2^2 \text{ and all } x_i \neq 0\}$$

which is a conic with six points removed. By the addition formula (3.3), these theta-constants $\theta_{a,b}$ are related to the theta-constants $\theta_{[0]}$ and $\theta_{[1]}$:

$$\begin{aligned}
\theta_{0,0}^2(0,\tau) &= \theta_{[0]}^2(0,\tau) + \theta_{[1]}^2(0,\tau), \\
\theta_{0,1}^2(0,\tau) &= \theta_{[0]}^2(0,\tau) - \theta_{[1]}^2(0,\tau), \\
\theta_{1,0}^2(0,\tau) &= 2\,\theta_{[0]}(0,\tau)\,\theta_{[1]}(0,\tau).
\end{aligned}$$

Hence one can express in a simple way the map Ψ thanks to the function Φ:

$$\Psi(\tau) = [1+\Phi^2(\tau)\,,\, 1-\Phi^2(\tau)\,,\, 2\Phi(\tau)],$$

for all τ in $\mathbb{H}$. □

Remark 3.13. Note that this identification of $X(4)$ is equivariant. More precisely, the finite group $G := \mathrm{PGL}(2, \mathbb{Z}/4\mathbb{Z})$ has cardinality 48 and acts by biholomorphisms or biantiholomorphisms on $X(4)$. The biholomorphism φ identifies this group G with the group of isometries of the octahedron. This follows from the identities

$$\Phi(-\overline{\tau}) = \overline{\Phi(\tau)} \ , \ \ \Phi(\tau+1) = \Phi(\tau) \text{ and } \ \Phi(-1/\tau) = \frac{-\Phi(\tau)+1}{\Phi(\tau)+1}\,.$$

3.5 Elliptic curves with complex multiplication

We can now go on the proof of Proposition 3.2, by explaining how we will check that a pair (λ, τ) satisfies Condition $(T_{\lambda,\tau})$.

For τ in $\mathbb{H}$, we introduce the lattice $\Lambda_\tau = \mathbb{Z}\tau \oplus \mathbb{Z}1$ of $\mathbb{C}$ so that the quotient $E_\tau := \mathbb{C}/\Lambda_\tau$ is the elliptic curve associated to τ. We will see that the values of λ and $\tau = \tau_{k,p}$ in Theorem 2.3 have been chosen so that the elliptic curve E_τ has complex multiplication by $\mu := \overline{\lambda}^2$. See [9] for more classical applications of complex multiplication. More precisely, they have been chosen so that $\mu\Lambda_\tau = \Lambda_{d^2\tau}$. This means that

$$d^2\tau \ = \ \mu\,(\alpha\tau+\beta), \tag{3.6}$$

$$1 \ = \ \mu\,(\gamma\tau+\delta), \tag{3.7}$$

for a matrix $\sigma = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$. We will be able to impose on σ the extra condition

$$\gamma > 0 \quad \text{and} \quad \sigma \equiv \pm\mathbb{1} \mod 4. \tag{3.8}$$

We explain why such a choice is relevant in the following lemma.

Lemma 3.14. *Let $\tau \in \mathbb{H}$ and d an odd integer.*
(a) The function θ_τ is (λ, d)-critical for some λ in $\mathbb{C}$ if and only if there exists $\sigma = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z})$ satisfying (3.8) such that $g\tau = d^2\tau$.
(b) In this case, the critical value is given by, setting $\mu = (\gamma\tau+\delta)^{-1}$,

$$\lambda = \varepsilon_\delta \left(\tfrac{\gamma}{\delta}\right) \overline{\mu}^{1/2}. \tag{3.9}$$

Recall that $\varepsilon_\delta = 1$ when $\delta \equiv 1 \mod 4$, and $\varepsilon_\delta = -i$ when $\delta \equiv 3 \mod 4$.

Proof of Lemma 3.14. (a) According to Lemma 3.11, the function θ_τ is (λ, d)-critical for some λ in $\mathbb{C}$ if and only if one has the equalities $\Phi(\tau) = \Phi(d^2\tau)$.

According to Lemma 3.12, this equality is equivalent to the existence of an element σ in $\Gamma(4)$ such that $\sigma\tau = d^2\tau$. Note that this forces the lower-left coefficient γ to be non zero. Replacing σ by $-\sigma$ if necessary, we can also assume that $\gamma > 0$.

(b) To compute the critical value λ, we use again Lemma 3.11 combined with Formulas (3.2). We obtain

$$\lambda = d\,\frac{\theta_{[0]}(0, d^2\tau)}{\theta_{[0]}(0,\tau)} = d\,\frac{\theta(0, d^2 2\tau)}{\theta(0, 2\tau)}\ .$$

Let $\sigma' = \begin{pmatrix} \alpha & \beta' \\ \gamma' & \delta \end{pmatrix}$, with $\beta' = 2\beta$, $\gamma' = \gamma/2$, so that $\sigma'(2\tau) = d^2 2\tau$. Since the matrix σ equals $\pm\mathbb{1}$ mod 4, the matrix σ' is equal to $\mathbb{1}$ mod 2. Hence we can apply the transformation formula in Lemma 3.8 to σ' and τ'. We get

$$\lambda = d\,\varepsilon_\delta \left(\tfrac{\gamma}{\delta}\right) (\gamma\tau + \delta)^{\frac{1}{2}}. \tag{3.10}$$

By assumption, the number $\mu := (\gamma\tau + \delta)^{-1}$ is a complex multiplication for the lattice Λ_τ, more precisely, one has $\mu\Lambda_\tau = \Lambda_{d^2\tau}$. This gives the equality $\mu\overline{\mu} = d^2$, and Equation (3.7) can be rewritten as

$$d^2\,(\gamma\tau + \delta) = \overline{\mu}.$$

Now Equation (3.10) can be rewritten as $\lambda = \varepsilon_\delta \left(\tfrac{\gamma}{\delta}\right) \overline{\mu}^{\frac{1}{2}}$. □

3.6 Choosing the elliptic curve

In order to end the proof of Proposition 3.2, it only remains to characterize those points τ in $\mathbb{H}$ that satisfy the condition $\sigma\tau = d^2\tau$ for some σ in $\Gamma(4)$ and to express the d-critical value λ given in Lemma 3.14 without using σ.

We begin by recalling the notation of Proposition 3.2. Let a, b be positive integers with $a \equiv \frac{(d+1)^2}{4}$ mod 4 and $a+b=d$. We introduced the "fundamental parameter" $\tau_0 := \frac{1}{4d^2}(a - b - d^2 + 2i\sqrt{ab}) \in \mathbb{H}$. For k in $\mathbb{Z}$, we introduced the integer $N_k := d^2|k + \tau_0|^2$. For $p \in \mathbb{N}$ dividing N_k, we also introduced the "associated parameters" $\tau_{k,p} := (k + \tau_0)/p \in \mathbb{H}$.

Lemma 3.15. *(a) Let τ in $\mathbb{H}$ such that there exists σ in $\Gamma(4)$ for which $\sigma\tau = d^2\tau$, then there exists k, p as above such that $\tau = \tau_{k,p}$ or $\tau = -\overline{\tau}_{k,p}$.*
(b) Conversely, for every $\tau = \tau_{k,p}$ as above, there exists σ in $\Gamma(4)$ such that $\sigma\tau = d^2\tau$.
(c) This matrix σ can be chosen to be $\sigma = \begin{pmatrix} 2(a-b)-d^2(1-4k) & -4N_k/p \\ 4p & 1-4k \end{pmatrix}$.

Proof. We first notice that, in this lemma, we can always add the extra conditions $\gamma > 0$ and $\sigma \equiv \mathbb{1} \bmod 4$. Indeed, if needed, we can always replace the matrix σ by $-\sigma$ without changing the point τ. We can also replace σ by the matrix $\begin{pmatrix} \alpha & -\beta \\ -\gamma & \delta \end{pmatrix}$, the point τ is then replaced by $-\overline{\tau}$.

(a) We set $\mu := (\gamma\tau+\delta)^{-1}$. Since the matrix $\sigma = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ has determinant 1, the equations (3.6) and (3.7) can be rewritten as

$$\begin{aligned} \gamma^{-1}(\mu^{-1} - \delta) &= \tau, & (3.11)\\ \mu^2 - t_0\mu + d^2 &= 0, & (3.12) \end{aligned}$$

with $t_0 := \alpha + d^2\delta$. We introduce a, b such that $t_0 = 2(a-b)$ and $d = a+b$.
$\star$ Since $\alpha \equiv \delta \equiv 1 \bmod 4$ and $d^2 \equiv 1 \bmod 4$, both numbers a and b are integers.
$\star$ Since μ is not a real number, one has $|t_0| < 2d$ and the integers a and b are positive.
$\star$ Since $\sigma \equiv \mathbb{1} \bmod 4$, one has $\alpha\delta \equiv 1 \bmod 16$, and these integers satisfy $a - b \equiv \frac{1+d^2}{2} \bmod 8$, and hence $a \equiv \frac{(d+1)^2}{4} \bmod 4$.
$\star$ Since $Im(\mu) < 0$, solving Equation (3.12), one gets the equality

$$\mu \;:=\; (\sqrt{a} - i\sqrt{b})^2 \;=\; a - b - 2i\sqrt{ab} \qquad (3.13)$$

$\star$ We write $\delta = 1 - 4k$ with $k \in \mathbb{Z}$, and one computes

$$\begin{aligned} N_k = d^2|k+\tau_0|^2 &= \tfrac{1}{16d^2}[((a-b)-(1-4k)d^2)^2 + 4ab] \\ &= \tfrac{1}{16}[1 - 2(a-b)(1-4k) + d^2(1-4k)^2] \\ &= (1-\alpha\delta)/16 \;=\; -\beta\gamma/16. \end{aligned}$$

$\star$ We write $\gamma = 4p$ so that this integer p is a divisor of the integer N_k.
$\star$ Plugging these informations in (3.11) gives $\tau = (k + \tau_0)/p$.

(b) and (c) We assume now that $\tau = \tau_{k,p}$ as above and we want to construct the matrix σ. We follow the same computation as in (a) in opposite

order. We set $\mu := a - b - 2i\sqrt{ab}$ and $t_0 := 2(a-b)$ so that Equation (3.12) is satisfied. We choose $\delta := 1 - 4k$ and $\alpha := t_0 - d^2\delta$. We first note that

$$\alpha\delta \equiv 1 \mod 16. \tag{3.14}$$

To check (3.14), just remember that one has $t_0 \equiv 1 + d^2 \bmod 16$, and hence

$$\alpha\delta - 1 \equiv (\delta - 1)(1 - \delta d^2) \equiv 4^2 \equiv 0 \mod 16.$$

Then the same computation as above gives the equality $(1 - \alpha\delta)/16 = N_k$. Hence if we choose $\gamma := 4p$ and $\beta := -4N_k/p$, the matrix σ is in $\Gamma(4)$. By construction these coefficients satisfy also Equality (3.11). Hence the matrix σ satisfies Equalities (3.6) and (3.7). □

Proof of Proposition 3.2. This proposition is now just a straightforward consequence of Lemmas 3.14 and 3.15 combined with Formula (3.13). □

3.7 Conclusion and Perspective

The aim of this paper was to explain why the algebraic integers $\sqrt{a} + i\sqrt{b}$ that occur in the lists of section 1.5 are indeed d-critical values when a, b are positive integers with $a + b = d$ and $a \equiv \frac{(d+1)^2}{4} \bmod 4$. To keep this paper as elementary as possible, we have only discussed here these d-critical values.

However, in the lists of section 1.5, there are still remaining intriguing d-critical values. In a more technical forthcoming paper [2], we will see that these d-critical values belong to a wide class of critical values on finite abelian groups that can be explained by an extension of the construction of Proposition 3.2. This will be a nice application of the abelian varieties and their theta funtions, relying on works of Siegel, Stark, Igusa and of Taniyama-Shimura. See [1] for a recent paper surveying previous applications of these tools. Indeed we will prove in [2].

Theorem 3.16. *Let $A = \mathbb{C}^g/\Lambda$ be a principally polarized abelian variety and ν be a unitary $\mathbb{Q}$-endomorphism of A preserving a theta structure of level 2. Let T_ν be its tangent map, G_ν the group $\Lambda/(\Lambda \cap T_\nu\Lambda)$ and d_ν the order of G_ν. Then there is a critical value $\lambda_\nu = \kappa_\nu\, d_\nu^{1/2} \det_{\mathbb{C}}(T_\nu)^{1/2}$ on G_ν with $\kappa_\nu^4 = 1$.*

Note that $|\lambda_\nu| = d_\nu^{1/2}$ and that one can compute the fourth root of unity κ_ν.

Note also that, any finite abelian group can occur as a group G_ν but, even when $g > 1$, this group G_ν may be cyclic. We will construct concrete examples with G_ν cyclic when the abelian variety A has complex multiplication. These constructions will explain all the intriguing d-critical values in our lists. For instance we will show in [2] by using abelian surfaces.

Corollary 3.17. *Let $d_j = a_j + b_j$ with $d_1 \wedge d_2 = 1$ and $a_j \equiv \frac{(d_j+1)^2}{4} + 2 \bmod 4$ be positive integers. Then $\lambda = (\sqrt{a_1} + i\sqrt{b_1})(\sqrt{a_2} - i\sqrt{b_2})$ is d-critical.*

Corollary 3.18. *Let $d = a+b+c$ be positive integers, with $b^2 > 4ac$, and $a \equiv b \equiv c \equiv 1$ mod 4. Then $\lambda = \sqrt{a} + \sqrt{c} + i\sqrt{b - 2\sqrt{ac}}$ is d-critical.*

A key remark in the proof of Corollary 3.18, is an old factorization formula:

$$\sqrt{a} + \sqrt{c} + i\sqrt{b - 2\sqrt{ac}} \;=\; \sqrt{a}\left(1 + i\sqrt{\tfrac{b+\sqrt{b^2-4ac}}{2a}}\right)\left(1 - i\sqrt{\tfrac{b-\sqrt{b^2-4ac}}{2a}}\right).$$

References

[1] A. Beauville. Theta functions, old and new. Surv. Mod. Math. 6, pages 99–132. Int. Press, 2013.

[2] Y. Benoist. Convolution and square in abelian groups II. hal-03744506 2022.

[3] C. Birkenhake and H. Lange. *Complex abelian varieties.* Grundlehren Math. 302. Springer, 2004.

[4] D. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms.* UTM. Springer, 1992.

[5] H. Farkas. Theta functions in complex analysis and number theory. In *Surveys in number theory, 17*, Dev. Math., pages 57–87. Springer, 2008.

[6] N. Koblitz. *Introduction to elliptic curves and modular forms.* GTM 97. Springer, 1984.

[7] D. Mumford. *Tata lectures on theta. I.* PM 28. Birkhäuser, 1983.

[8] H. Rademacher. *Topics in analytic number theory.* GMW 169. Springer, 1973.

[9] R. Schertz. *Complex multiplication.* NMM 15. Cambridge Univ. Press, 2010.

Y. Benoist: CNRS, Université Paris-Saclay, yves.benoist@u-psud.fr