arXiv:1011.0914v1 [math.NT] 3 Nov 2010

The complex AGM, periods of elliptic curves over $\mathbb{C}$ and complex elliptic logarithms

John E. Cremona
Thotsaphon Thongjunthug

November 4, 2010

Abstract

We present a method for computing period lattices and elliptic logarithms for elliptic curves defined over $\mathbb{C}$, using the complex Arithmetic-Geometric Mean (AGM) first studied by Gauss. Earlier authors have only considered the case of elliptic curves defined over the real numbers; here, the multi-valued nature of the complex AGM plays an important role. Our method, which we have implemented in both MAGMA and Sage, is illustrated with several examples.

1 Introduction

Let E be an elliptic curve defined over $\mathbb{C}$, given by a Weierstrass equation

$$E: \quad Y^2 = 4(X-e_1)(X-e_2)(X-e_3),$$

where the roots $e_j \in \mathbb{C}$ are distinct. As is well known, there is an isomorphism (of complex analytic Lie groups) $\mathbb{C}/\Lambda \cong E(\mathbb{C})$, where Λ is the *period lattice* of E: specifically, we take Λ to be the lattice of periods of the invariant differential dX/Y on E. It is a discrete rank 2 subgroup of $\mathbb{C}$, spanned by a $\mathbb{Z}$-basis $\{w_1, w_2\}$ with $w_2/w_1 \notin \mathbb{R}$. The isomorphism is given by the map

$$z \pmod{\Lambda} \mapsto P = (\wp_\Lambda(z), \wp'_\Lambda(z)) \in E(\mathbb{C})$$

(with $0 \pmod{\Lambda} \mapsto O \in E(\mathbb{C})$, the base point at infinity) where $\wp_\Lambda$ denotes the classical elliptic Weierstrass function associated to the lattice Λ. The inverse of this map,

$$P \mapsto z \pmod{\Lambda},$$

from $E(\mathbb{C})$ to $\mathbb{C}/\Lambda$, is called the *elliptic logarithm*, and we say that any $z \in \mathbb{C}$ representing its class modulo Λ is an *elliptic logarithm* of P. Two natural questions are:

1. How can we compute a basis for the period lattice Λ of E, given a Weierstrass equation?
2. Given a point $P = (x, y) \in E(\mathbb{C})$, how can we compute its elliptic logarithm $z \in \mathbb{C}$?

For elliptic curves over $\mathbb{R}$, these questions have been answered satisfactorily and are well-known. Algorithms for computing $\mathbb{Z}$-bases for period lattices of elliptic curves defined over $\mathbb{R}$, and elliptic logarithms of real points on such curves, may be found in the literature (see, for example, [3, Algorithm 7.4.8] or [5, §3.7]). These use the real *arithmetic-geometric mean* (AGM), and allow one to compute both values rapidly with a high degree of precision. The theory behind this method is described succinctly by Mestre in [2]. The situation for elliptic curves over $\mathbb{C}$, however, is less satisfactory.

In this paper, we will give a complete method for computing period lattices and elliptic logarithms for elliptic curves over $\mathbb{C}$, by generalising the real algorithm. To this end, we will first explain the connection between the following three classes of objects:

- Complex AGM sequences, as first studied by Gauss and explored in depth more recently by Cox [4];
- Chains of lattices in $\mathbb{C}$;
- Chains of 2-isogenies between elliptic curves defined over $\mathbb{C}$.

These will be defined precisely below. This connection will allow us to derive an explicit formula (see Theorems 19 and 21 below), based on so-called *optimal* complex AGM values, for a $\mathbb{Z}$-basis of the period lattice of any elliptic curve defined over $\mathbb{C}$. We then develop our method further to give an iterative method (Algorithm 28) for computing elliptic logarithms of complex points.

Our approach to the computation of periods follows closely that of Bost and Mestre [2] in the real case. However, in that case there is only a single chain of 2-isogenies which needs to be considered, and a unique AGM sequence, while over $\mathbb{C}$ we find it convenient to consider a whole class of such sequences. The connection between these three types of sequence has some independent interest.

We note that the recent paper by Dupont [6] also presents related methods for evaluating modular functions using the complex AGM, including explicit complexity results. The results in [6] may also be used to compute complex periods, as these are given by elliptic integrals with complex parameters.

In the next three sections of the paper we consider in turn complex AGM sequences (as are described well in Cox [4]), then lattice chains and finally chains of 2-isogenies. Then we give the first application, to the computation of a basis for the period lattice (see Theorem 21). The following section gives a new proof of a result about the complete set of values of the (multi-valued) complex AGM, slightly more general than the version in [4]. Then in Section 8 we develop the elliptic logarithm algorithm (Algorithm 28). The paper ends with a set of illustrative examples.

Our algorithms have been implemented by the authors both in Sage (see [8]) and in MAGMA (see [1], code available from the second author).

The results of this paper form part of the PhD thesis [9] of the second author. The proofs are in some cases different: in [9] both the periods and elliptic logarithms are expressed more traditionally, as integrals over the Riemann surface $E(\mathbb{C})$; however the resulting iterative algorithms are identical. The second author acknowledges the support of the Development and Promotion of Science and Technology Talent Project (DPST) of the Ministry of Education, Thailand.

2 AGM Sequences

Let $(a,b) \in \mathbb{C}^2$ be a pair of complex numbers satisfying

$$a \neq 0, \quad b \neq 0, \quad a \neq \pm b. \tag{1}$$

We say that (a,b) is *good* if $\Re(b/a) \geq 0$, or equivalently,

$$|a-b| \leq |a+b|; \tag{2}$$

otherwise the pair is said to be *bad*. Clearly, only one of the pairs (a,b), $(a,-b)$ is good, unless $\Re(b/a) = 0$ (or equivalently, $|a-b| = |a+b|$), in which case both are good.

An *arithmetic-geometric mean* (AGM) *sequence* is a sequence $((a_n,b_n))_{n=0}^{\infty}$, whose pairs $(a_n,b_n) \in \mathbb{C}^2$ satisfy the relations

$$2a_{n+1} = a_n + b_n, \quad b_{n+1}^2 = a_n b_n$$

for all $n \geq 0$. It is easy to see that if any one pair (a_n,b_n) in the sequence satisfies (1) then all do, and we will make this restriction henceforth.

From any given starting pair (a_0,b_0) there are uncountably many AGM sequences, obtained by iterating the procedure of replacing (a_n,b_n) by the arithmetic mean $a_{n+1} = (a_n+b_n)/2$ and the geometric mean $b_{n+1} = \sqrt{a_n b_n}$, with a choice of the square root for b_{n+1} at each step. However, we usually prefer to consider the entire sequence as a whole. We say that an AGM sequence is *good* if the pairs (a_n,b_n) are good for all but finitely many n. A good AGM sequence in which (a_n,b_n) are good for all $n > 0$ is said to be *optimal*, and *strongly optimal* if in addition (a_0,b_0) is good. If an AGM sequence is not good, then we say that it is *bad*.

It is easy to check that $(a_{n+1}, \pm b_{n+1})$ are both good if and only if a_n/b_n is real and negative, in which case (a_n,b_n) is certainly bad. In an optimal sequence, this situation can only occur for $n = 0$. In consequence, for every starting pair (a_0,b_0) there is exactly one optimal AGM sequence, unless a_0/b_0 is real and negative, in which case there are two, with different signs of b_1, with the property that the ratios a_n/b_n in one of the sequences are the complex conjugates of those in the other.

The following proposition is from Cox (see [4]); the proof of parts (1) and (2) is elementary, and we refer the reader to [4]; part (3) appears deeper, and we will give a proof below after relating the different AGM values to a certain set of periods of an elliptic curve. Note that Cox defines the notion of "good" more strictly than above (when $\Re(a/b) = 0$ he requires $\Im(a/b) > 0$, so that exactly one of $(a, \pm b)$ is good in every case), but in view of the preceding remarks this does not affect the following result.

Proposition 1. *Given a pair $(a_0,b_0) \in \mathbb{C}^2$ satisfying* (1)*, every AGM sequence $((a_n,b_n))_{n=0}^{\infty}$ starting at (a_0,b_0) satisfies the following:*

1. $\lim_{n\to\infty} a_n$ *and* $\lim_{n\to\infty} b_n$ *exist and are equal;*
2. *The common limit, say M, is non-zero if and only if the sequence is good;*
3. $|M|$ *attains its maximum (among all AGM-sequences starting at (a_0,b_0)) if and only if the sequence is optimal.*

For an AGM sequence $((a_n, b_n))_{n=0}^{\infty}$ starting at (a_0, b_0), we will denote the common limit $\lim_{n\to\infty} a_n = \lim_{n\to\infty} b_n$ by $M_S(a_0, b_0)$, where $S \subseteq \mathbb{Z}_{>0}$ is the set of all indices n for which the pair (a_n, b_n) is bad. For example, $M_\emptyset(a_0, b_0)$ denotes the common limit for the optimal AGM sequence. To avoid ambiguities when a_0/b_0 is negative real, we may agree to choose b_1 so that $\Im(a_1/b_1) > 0$ in that case, though this choice will not affect our results below. Note that the AGM sequence is good if and only if S is a finite set. To ease notation, we shall write $M_\emptyset(a_0, b_0)$ simply as $M(a_0, b_0)$.

3 Lattice Chains

In this paper, a *lattice* will always be a free $\mathbb{Z}$-module of rank 2, embedded as a discrete subgroup of $\mathbb{C}$. Elements of lattices will often be called periods, since in our application the lattices will arise as period lattices of elliptic curves defined over $\mathbb{C}$.

The following definition, as well as Lemma 2, only depend on the algebraic structure of lattices. We define a *chain of lattices (of index* 2*)* to be a sequence of lattices $(\Lambda_n)_{n=0}^{\infty}$ which satisfies the following conditions:

1. $\Lambda_n \supset \Lambda_{n+1}$ for all $n \geq 0$;
2. $[\Lambda_n : \Lambda_{n+1}] = 2$ for all $n \geq 0$;
3. Λ_0/Λ_n is cyclic for all $n \geq 1$; equivalently, $\Lambda_{n+1} \neq 2\Lambda_{n-1}$ for all $n \geq 1$.

Thus for each $n \geq 1$ we have

$$\Lambda_{n+1} = \langle w \rangle + 2\Lambda_n \tag{3}$$

for some $w \in \Lambda_n \setminus 2\Lambda_{n-1}$. Given an initial lattice Λ_0, there are three possibilities for Λ_1. When $n \geq 1$, one of the three sublattices of index 2 is excluded, since it is contained in $2\Lambda_{n-1}$ (which would contradict the last condition in the definition), and so there are only two possible choices for Λ_{n+1}. The number of such chains starting with Λ_0 is uncountable; we will distinguish a countable subset of these as follows. Let

$$\Lambda_\infty = \bigcap_{n=0}^{\infty} \Lambda_n.$$

Then Λ_∞ is free of rank at most 1; the rank cannot be 2, since for all n,

$$[\Lambda_0 : \Lambda_\infty] \geq [\Lambda_0 : \Lambda_n] = 2^n,$$

so $[\Lambda_0 : \Lambda_\infty]$ is infinite. We say that the chain is *good* if Λ_∞ has rank 1; in this case a generator for Λ_∞ will be called a *limiting period* of the chain. We will first show that the limiting period is *primitive*, i.e. not in $m\Lambda_0$ for any $m \geq 2$.

Lemma 2. *Let $(\Lambda_n)_{n=0}^{\infty}$ be a good chain with $\Lambda_\infty = \langle w_\infty \rangle$. Then*

1. *w_∞ is primitive; equivalently, Λ_0/Λ_∞ is free of rank 1;*
2. *$\Lambda_n = \langle w_\infty \rangle + 2^n \Lambda_0$ for all $n \geq 0$.*

Proof. Suppose that $w_\infty = mw$ for some $m \geq 1$ and $w \in \Lambda_0$. If m is odd, then since Λ_0/Λ_n has order 2^n which is prime to m, we see that

$$mw \in \Lambda_n \implies w \in \Lambda_n$$

for all n, so that $w \in \Lambda_\infty$. Hence (by definition of w_∞), $m = 1$.

Next suppose that $w_\infty = 2w$ for some $w \in \Lambda_0$. By definition of w_∞, we then have $w \notin \Lambda_\infty$, and hence there exists $n > 0$ such that $w \notin \Lambda_n$. This implies that $w_\infty \in \Lambda_n \setminus 2\Lambda_n$. But since $w_\infty \in \Lambda_{n+1}$, we have

$$\Lambda_{n+1} = \langle w_\infty \rangle + 2\Lambda_n = \langle 2w \rangle + 2\Lambda_{n+1} \subseteq 2\Lambda_0,$$

which contradicts the definition of a chain. This proves the first statement.

The second statement follows from the fact that $\Lambda_n/2^n\Lambda_0$ is cyclic of order 2^n, and is generated by w_∞ modulo $2^n\Lambda_0$, since w_∞ is primitive. □

So far, our notion of a good chain has been defined as a property of the chain as a whole, and only used the abstract structure of lattices as free $\mathbb{Z}$-modules. Using the next definition, we will see that this property can also be seen in terms of the individual steps $\Lambda_n \supset \Lambda_{n+1}$, when the lattices are embedded in $\mathbb{C}$. In view of (3), the choice of Λ_{n+1} is determined by the class of w modulo $2\Lambda_n$.

For $n \geq 1$, we say that $\Lambda_{n+1} \subset \Lambda_n$ is the *right choice* of sublattice of Λ_n if $\Lambda_{n+1} = \langle w \rangle + 2\Lambda_n$ where w is a *minimal* element in $\Lambda_n \setminus 2\Lambda_{n-1}$ (with respect to the usual complex absolute value).

Lemma 3. *Let $(\Lambda_n)_{n=0}^\infty$ be a good chain with $\Lambda_\infty = \langle w_\infty \rangle$. Then w_∞ is minimal in Λ_n for all but finitely many $n \geq 0$.*

Proof. Since Λ_0 is discrete, the number of periods $w \in \Lambda_0$ with $0 < |w| < |w_\infty|$ is finite. Each of these periods lies in only finitely many Λ_n by minimality of w_∞ in Λ_∞, so there exists n_0 such that w_∞ is minimal in Λ_{n_0} and hence also in Λ_n for all $n \geq n_0$. □

The following proposition yields an alternative notion of a good chain. For now we remark that this is analogous to the definition of a good AGM sequence in the previous section; more of its analogues will be seen in later sections.

Proposition 4. *A chain of lattices $(\Lambda_n)_{n=0}^\infty$ is good if and only if $\Lambda_{n+1} \subset \Lambda_n$ is the right choice for all but finitely many $n \geq 1$.*

Proof. Let $(\Lambda_n)_{n=0}^\infty$ be a good chain with $\Lambda_\infty = \langle w_\infty \rangle$. Then by Lemma 3, there exists an integer n_0 such that w_∞ is minimal in Λ_n for all $n \geq n_0$. Since $\Lambda_{n+1} = \langle w_\infty \rangle + 2\Lambda_n$ for all n, then by definition, $\Lambda_{n+1} \subset \Lambda_n$ is the right choice for all $n \geq n_0$.

Conversely, suppose that $\Lambda_{n+1} \subset \Lambda_n$ is the right choice for all $n \geq n_0$ (where $n_0 \geq 1$). Without loss of generality, we may suppose that $n_0 = 1$. Let $w_1 \in \Lambda_1$ be a minimal element. Then w_1 is certainly primitive (as an element of Λ_1, though not necessarily in Λ_0). We claim that $w_1 \in \Lambda_n$ for all $n \geq 1$, so that the chain is good with limiting period w_1.

To prove the claim, suppose that $w_1 \in \Lambda_j$ for all $j \leq n$. Then $\Lambda_n = \langle w_1 \rangle + 2^{n-1}\Lambda_1$, since the latter is contained in the former and both have index 2^{n-1} in Λ_1. Hence $\Lambda_n = \langle w_1, 2^{n-1}w_2 \rangle$, where $w_2 \in \Lambda_1$ is such that $\Lambda_1 = \langle w_1, w_2 \rangle$. The right sublattice of Λ_{n+1} is clearly $\langle w_1 \rangle + \Lambda_n$, by minimality of w_1 (which is a candidate since $w_1 \in \Lambda_n \setminus 2\Lambda_{n-1}$); in particular, $w_1 \in \Lambda_{n+1}$, as required. □

3.1 Optimal Chains and Rectangular Lattices

Let us define a lattice chain to be *optimal* if $\Lambda_{n+1} \subset \Lambda_n$ is the right choice for *all* $n \geq 1$. We will see that there is in general just one optimal chain for each of the three choices of $\Lambda_1 \subset \Lambda_0$. In order to make the statement more precise, however, some preparation is necessary.

We say that a lattice $\Lambda \subset \mathbb{C}$ is *rectangular* if it has an "orthogonal" $\mathbb{Z}$-basis $\{w_1, w_2\}$, i.e. one which satisfies $\Re(w_2/w_1) = 0$. For example, the period lattice of an elliptic curve defined over $\mathbb{R}$ with positive discriminant is rectangular, where an orthogonal basis is given by the least real period and the least imaginary period. In general, rectangular lattices are homothetic to the period lattices of this family of elliptic curves.

If $\{w_1, w_2\}$ is any $\mathbb{Z}$-basis for a lattice Λ, the three non-trivial cosets of 2Λ in Λ are $C_j = w_j + 2\Lambda$ for $j = 1, 2, 3$, where $w_3 = w_1 + w_2$. By a *minimal coset representative* in Λ we mean a minimal element of one of these cosets. Minimal coset representatives are always primitive; for they are certainly not in 2Λ, and if $w = mw'$ with $m \geq 3$ odd, then $|w'| < |w|$ while w' is in the same coset as w.

Lemma 5. *In each coset C_j the minimal coset representative is unique up to sign, except in the case of a rectangular lattice with orthogonal basis $\{w_1, w_2\}$ where the coset C_3 has four minimal vectors, $\pm(w_1 \pm w_2)$.*

Proof. For a rectangular lattice with orthogonal basis $\{w_1, w_2\}$, it is easy to see that the minimal coset representatives are as stated. Conversely, suppose that the lattice Λ has a coset C with at least two pairs of minimal elements, $\pm w$ and $\pm w'$. Then $w_1, w_2 = (w \pm w')/2 \in \Lambda$ are easily seen to be orthogonal.

If $w_1 \equiv 0 \pmod{2\Lambda}$, then $w_2 \equiv w \pmod{2\Lambda}$. But then $|w_2| < |w_1 + w_2| = |w|$, contradicting minimality of w in its coset. Hence $w_1 \not\equiv 0 \pmod{2\Lambda}$. Similarly, $w_2 \not\equiv 0 \pmod{2\Lambda}$. Moreover, $w_1 \not\equiv w_2 \pmod{2\Lambda}$ since $w = w_1 + w_2 \equiv w_1 - w_2 \not\equiv 0 \pmod{2\Lambda}$. Therefore, w_1, w_2, w do represent the three non-trivial cosets modulo 2Λ. Now if $\{w_1, w_2\}$ was not a $\mathbb{Z}$-basis, there would exist a non-zero period $w_0 = \alpha w_1 + \beta w_2$ with $0 \leq \alpha, \beta < 1$. But then one of $w_0, w_0 - w_1, w_0 - w_2, w_0 - w$ is in the same coset as w, and all are smaller, contradiction. □

Our algorithm for computing periods of elliptic curves will in fact compute minimal coset representatives. Although these are individually primitive, to ensure that we thereby obtain a $\mathbb{Z}$-basis for the lattice, the following lemma is required.

Lemma 6. *For $j = 1, 2, 3$, let w_j be minimal coset representatives for a non-rectangular lattice $\Lambda \subset \mathbb{C}$; that is, minimal elements of the three non-trivial cosets of 2Λ in Λ. Then any two of the w_j form a $\mathbb{Z}$-basis for Λ, and $w_3 = \pm(w_1 \pm w_2)$.*

Proof. We may assume that $|w_1| \leq |w_2| \leq |w_3|$. Then w_1 is minimal in Λ and w_2 is minimal in $\Lambda \setminus \langle w_1 \rangle$. Hence (replacing w_2 by $-w_2$ if necessary) $\tau = w_2/w_1$ is in the standard fundamental region for $\mathrm{SL}_2(\mathbb{Z})$ acting on the upper half-plane, $\{w_1, w_2\}$ is a $\mathbb{Z}$-basis, and $w_3 = w_2 \pm w_1$; the sign depends on that of $\Re(\tau)$. □

The following proposition shows that the limiting period of an optimal chain is closely related to minimal coset representatives.

Proposition 7. *A good chain of lattices $(\Lambda_n)_{n=0}^{\infty}$ with $\Lambda_\infty = \langle w_\infty \rangle$ is optimal if and only if w_∞ is a minimal coset representative of $2\Lambda_0$ in Λ_0.*

Proof. Suppose that w_∞ is a minimal coset representative. Then it is clear that $\Lambda_{n+1} = \langle w_\infty \rangle + 2\Lambda_n \subset \Lambda_n$ is the right sublattice for all $n \geq 1$, since w_∞ is certainly minimal in $\Lambda_n \setminus 2\Lambda_{n-1}$.

Conversely, suppose that the sequence is optimal. Let w be a minimal element of $\Lambda_1 \setminus 2\Lambda_0$, so that w is a minimal coset representative for the unique non-trivial coset of $2\Lambda_0$ which is contained in Λ_1. Note that w is unique up to sign, unless Λ_0 is rectangular in which case (for one of the cosets) there will be two possibilities for w up to sign. By optimality, the sublattice $\Lambda_2 \subset \Lambda_1$ is the right choice. In particular, if Λ_0 is not rectangular, then we must therefore have $\Lambda_2 = \langle w \rangle + 2\Lambda_1$. This, however, may not hold in the rectangular case, but it will hold if we replace w by the other choice of minimal coset representative.

Now we claim that $\Lambda_n = \langle w \rangle + 2\Lambda_{n-1}$ for all $n \geq 2$. We already know this for $n = 2$. If the claim is true for n, then certainly $w \in \Lambda_n \setminus 2\Lambda_{n-1}$ (since $w \notin 2\Lambda_0$), so the (unique) good choice of sublattice of Λ_n is $\langle w \rangle + 2\Lambda_n$. By optimality, this is Λ_{n+1}, and so the claim holds for $n+1$. Thus $w \in \bigcap_{n=0}^{\infty} \Lambda_n = \langle w_\infty \rangle$, and indeed, $w = \pm w_\infty$, since w is primitive. □

Combining Lemma 5 with Proposition 7, we have the following conclusion.

Corollary 8. *Every non-rectangular lattice Λ has precisely three optimal sublattice chains, whose limiting periods are the minimal coset representatives in each of the three non-zero cosets of 2Λ in Λ. Every rectangular lattice Λ has precisely four optimal sublattice chains.*

4 Short lattice chains and level 4 structures

In this section we establish a link between AGM sequences and lattice chains. The first step is to associate a pair of nonzero complex number (a, b) (with $a \neq \pm b$) to each "short" lattice chain $\Lambda_0 \supset \Lambda_1 \supset \Lambda_2$ in such a way that (a, b) is good in the sense of Section 2 if and only if Λ_2 is the right choice of sublattice of Λ_1, in the sense of Section 3.

We establish bijections between the following sets:

1. "short" lattice chains $\Lambda_0 \supset \Lambda_2$ with Λ_0/Λ_2 cyclic of order 4;
2. triples (E, ω, H) where E is an elliptic curve defined over $\mathbb{C}$, ω a holomorphic differential on E, and $H \subset E(\mathbb{C})$ a cyclic subgroup of order 4;
3. unordered pairs of nonzero complex numbers a, b with $a^2 \neq b^2$, where the pairs a, b and $-a, -b$ are identified.

For each short lattice chain $\Lambda_0 \supset \Lambda_2$, if we set $\Lambda_1 = \Lambda_2 + 2\Lambda_0$ then $(\Lambda_0, \Lambda_1, \Lambda_2)$ satisfy the conditions for the first three terms in a lattice sequence as defined earlier. Hence we will usually think of a short lattice chain as a triple $\Lambda_0 \supset \Lambda_1 \supset \Lambda_2$, even though Λ_1 is uniquely determined by the other two.

To each short lattice chain we associate the elliptic curve $E = \mathbb{C}/\Lambda_0$ with differential $\omega = dz$ and subgroup $H = (1/4)\Lambda_2/\Lambda_0$. Conversely, to a triple (E, ω, H) we associate the chain $\Lambda_0 \supset \Lambda_2$ where Λ_0 is the lattice of periods of ω

(so that $E(\mathbb{C}) \cong \mathbb{C}/\Lambda_0$), and Λ_2 is the sublattice such that $H \cong (1/4)\Lambda_2/\Lambda_0$ under this isomorphism.

Each triple (E, ω, H) has a model of the form

$$E_{\{a,b\}}: \quad Y^2 = 4X(X + a^2)(X + b^2),$$

for some unordered pair $a, b \in \mathbb{C}^*$ such that $a^2 \neq b^2$, where $\omega = dX/Y$, and H is the subgroup generated by the point

$$P_{\{a,b\}} = (ab, 2ab(a + b)).$$

The four points $P_{\{\pm a,\pm b\}}$ are the solutions to $2P = T = (0, 0) \in E_{\{a,b\}}(\mathbb{C})[2]$. Interchanging $\{a, b\}$ and $\{-a, -b\}$ does not affect the curve and interchanges $P_{\{a,b\}}$ and $P_{\{-a,-b\}} = -P_{\{a,b\}}$ so does not change H. On the other hand, changing the sign of just one of a, b changes H to the other cyclic subgroup of order 4 containing T. Hence the pair $\{a, b\}$ has the properties stated and is well-defined up to changing the signs of both a and b,

Conversely, given $\{a, b\}$ with $ab \neq 0$ and $a \neq \pm b$, we recover the triple $(E_{\{a,b\}}, \omega, H)$, which is unchanged by either interchanging a and b or negating both.

If we only consider elliptic curves up to isomorphism, we may ignore the differential ω, scale the equations arbitrarily, and consider lattices only up to homothety. Now we can identify pairs $\{a, b\}$ and $\{ua, ub\}$ for all $u \in \mathbb{C}^*$. The equation for $E_{\{a,b\}}$ can be scaled so that $ab = 1$, giving the homogeneous form

$$E_f: \quad Y^2 = 4X(X^2 + fX + 1),$$

where

$$f = \frac{a^2 + b^2}{ab} = \frac{a}{b} + \frac{b}{a} \neq \pm 2.$$

In this model, the points $\pm P_{\{a,b\}}$ generating the distinguished subgroup H now have coordinates $(1, \pm 2\sqrt{2 + f})$. Thus the pair E, H uniquely determines a complex number $f \in \mathbb{C} \setminus \{\pm 2\}$. We call this f the *modular parameter* for the level 4 structure, since (as we will see below) it is in fact the value of a modular function for the congruence subgroup $\Gamma_0(4)$.

Proposition 9. *The above constructions give a bijection between these sets:*

1. *"short" lattice chains $\Lambda_0 \supset \Lambda_2$ up to homothety;*
2. *pairs (E, H) where E is an elliptic curve defined over $\mathbb{C}$ with $H \subset E(\mathbb{C})$ a distinguished cyclic subgroup of order 4, up to isomorphism (where isomorphisms preserve the distinguished subgroups);*
3. *complex numbers $f \in \mathbb{C} \setminus \{\pm 2\}$.*
4. *points in the open modular curve $Y_0(4) = \Gamma_0(4)\backslash\mathcal{H}$, where $\mathcal{H}$ denotes the upper half-plane.*

Remark. It would appear that considering pairs (E, P), where P is a point of exact order 4 in $E(\mathbb{C})$, would give a refinement to the level 4 structure, corresponding to points on the modular curve $Y_1(4) = \Gamma_1(4)\backslash\mathcal{H}$, since $[\Gamma_0(4) : \Gamma_1(4)] = 2$. However, this is an illusion: since every E has an automorphism $[-1]$ which takes P to $-P$, the set of pairs (E, H) (up to isomorphism) may be identified with the space of pairs (E, P) (also up to isomorphism). Similarly, since $\Gamma_0(4) = (\pm I)\Gamma_1(4)$, we may identify $Y_1(4)$ and $Y_0(4)$.

Proof. Bijections between all sets except the last have already been established.

Up to homothety, the lattice Λ_0 is determined by $\tau \in \mathcal{H}$ modulo the action of the modular group $\Gamma = \mathrm{SL}(2, \mathbb{Z})$: for any oriented basis w_1, w_2 of Λ_0 (where "oriented" means $w_2/w_1 \in \mathcal{H}$) we associate $\tau = w_2/w_1 \in \mathcal{H}$. All oriented bases w_1', w_2' of Λ_0 have the form

$$\begin{aligned} w_2' &= aw_2 + bw_1 \\ w_1' &= cw_2 + dw_1 \end{aligned}$$

with[1] $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, and $\tau' = w_2'/w_1' = (a\tau + b)/(c\tau + d)$. To allow for the additional level 4 structure, we restrict to oriented bases w_1, w_2 such that $\Lambda_2 = \langle w_1 \rangle + 4\Lambda_0$, so that w_1', w_2' is only admissible if $w_1 \equiv \pm w_1' \pmod{4\Lambda_0}$, or equivalently $(c, d) \equiv (0, \pm 1) \pmod 4$. This uniquely determines the $\Gamma_0(4)$-orbit of τ and not just its Γ-orbit.

Let $Y_0(4) = \Gamma_0(4)\backslash\mathcal{H}$ denote the open modular curve associated to $\Gamma_0(4)$, and $X_0(4)$ its completion, obtained by including the three cusps (represented by ∞, 0 and $1/2 \in \mathbb{P}^1(\mathbb{Q})$), which has genus 0. Hence the function field of $X_0(4)$ is generated by a single function. Since the j-invariant of E_f is $256(f^2 - 3)^3/(f^2 - 4)$, we see that $f = f(\tau)$ is a suitable function. This establishes the claim concerning f, and completes the proof of the proposition. ☐

Remark. There is an involution on each of these sets, which preserves the level 2 structure but interchanges the two possible associated level 4 structures. In each of the sets this takes the following forms: replace Λ_2 by the other sublattice Λ_2' of index 2 in Λ_1 such that Λ_0/Λ_2' is cyclic; replace H by the other subgroup H' which is cyclic of order 4 and contains $T = (0, 0)$; change the sign of one of a, b; or change f to $-f$. This involution comes from the nontrivial automorphism of the cover $X_0(4) \to X_0(2)$ of degree 2; the function field of $X_0(2)$ is generated by f^2.

Remark. Since $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \Gamma_0(4) \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}^{-1} = \Gamma(2)$, the function field of $X_0(4)$ may also be generated by $\lambda(2\tau)$ where $\lambda(\tau)$ is the classical Legendre elliptic function which generates the function field of $X(2)$. A calculation shows that $f(\tau) = 2(1 + \lambda(2\tau))/(1 - \lambda(2\tau))$. One interpretation of this is that instead of parametrizing short lattice chains by the parameter $\tau \in Y_0(4)$ corresponding to Λ_0 with $\Gamma_0(4)$-structure, we could instead have used the parameter $2\tau \in Y(2)$ to parametrize the middle lattice Λ_1 with full level 2-structure given by the sublattices $\frac{1}{2}\Lambda_0$ and Λ_2.

We now state the main result of this section.

Theorem 10. *Let $\Lambda_0 \supset \Lambda_1 \supset \Lambda_2$ be a short lattice chain corresponding to the unordered pair $\{a, b\}$ and modular parameter f. Then the following are equivalent:*

1. *Λ_2 is the right choice of sublattice of Λ_1;*
2. *the pair (a, b) is good;*
3. *$\Re(f) \geq 0$.*

[1] The reason for ordering bases this way is to maintain consistency with other sections.

Proof. Equivalence of the second and third conditions is immediate from $f = a/b+b/a$ since (a,b) is good if and only if $\Re(a/b) \geq 0$. (In terms of the Legendre function, the equivalent condition is that $|\lambda(2\tau)| \leq 1$.)

For equivalence of the first condition, we need to work harder. Recall that Λ_2 is the right choice of sublattice if $\Lambda_2 = \langle w_1 \rangle + 2\Lambda_1 = \langle w_1 \rangle + 4\Lambda_0$, where w_1 is the minimal period in its coset modulo $2\Lambda_1$. We now characterize this condition in terms of the imaginary part of $\tau \in \mathcal{H}$.

Lemma 11. *Let w_1, w_2 be any oriented basis for Λ_0 such that $\Lambda_2 = \langle w_1 \rangle + 4\Lambda_0$, and let $\tau = w_2/w_1$. The following are equivalent:*

1. *$\Im\tau$ is maximal, over all τ in its $\Gamma_0(4)$-orbit;*
2. *$|c\tau + d| \geq 1$ for all coprime $c, d \in \mathbb{Z}$ such that $(c,d) \equiv (0, \pm 1) \pmod 4$;*
3. *$|w_1|$ is minimal, over all primitive periods of Λ_0 such that $\Lambda_2 = \langle w_1 \rangle + 4\Lambda_0$;*
4. *$|\tau + d/4| \geq 1/4$ for all odd $d \in \mathbb{Z}$.*

Proof. Equivalence of the first two statements follows from $\Im(\gamma\tau) = \Im\tau/|c\tau+d|^2$ for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Since $|c\tau+d| \geq 1 \iff |cw_2+dw_1| \geq |w_1|$, the third statement is also equivalent to these. For the last statement, consider the geometry of the upper half-plane: the region given by these conditions are the same: (4) states that τ lies on or above all the semicircles centred on rationals with denominator 4 and with radius $1/4$, while (2) says that τ lies above all semicircles centred at rationals $-d/c$ with radius $1/c$ for which $(c,d) \equiv (0, \pm 1) \pmod 4$; as the semicircles for $c > 4$ lie strictly under those for $c = 4$, this is no stronger. ☐

We denote by $\mathcal{F}(4)$ the set of τ which satisfy these conditions; that is, those for which $\Im\tau$ is maximal in a $\Gamma_0(4)$-orbit. The subset of $\mathcal{F}(4)$ consisting of τ such that $0 \leq \Re\tau \leq 1$ is a (closed) fundamental region for $\Gamma_0(4)$. Since $\Gamma_0(4)$ has index 2 in $\Gamma_0(2)$, the region $\mathcal{F}(4)$ decomposes into two components, which we denote $\mathcal{F}^{\pm}(4)$: the first is $\mathcal{F}^{+}(4) = \mathcal{F}(2)$, consisting of all τ lying on or above all semicircles of radius $1/2$ centred at rationals with denominator 2; a closed fundamental region for $\Gamma_0(2)$ is the subset of $\mathcal{F}(2)$ consisting of τ such that $0 \leq \Re\tau \leq 1$. Secondly, $\mathcal{F}^{-}(4) = \overline{\mathcal{F}(4) \setminus \mathcal{F}(2)}$. The boundary between these is $\mathcal{F}^{+}(4) \cap \mathcal{F}^{-}(4)$, which consists of the union of the semicircles $|\tau + d/2| = 1/2$ for all odd $d \in \mathbb{Z}$.

The lemma above shows that Λ_2 is the right choice if and only if the τ for which $\Im\tau$ is maximal over all τ in its $\Gamma_0(4)$-orbit is also maximal in the larger $\Gamma_0(2)$-orbit; in other words, given that $\tau \in \mathcal{F}(4)$, we in fact have $\tau \in \mathcal{F}^{+}(4)$.

The following lemma then completes the proof of the theorem. ☐

Lemma 12. *Let $\tau \in \mathcal{F}(4)$. Then*

$$\Re f(\tau) \geq 0 \iff \tau \in \mathcal{F}^{+}(4).$$

Proof. This will follow by continuity from the following facts, for $\tau \in \mathcal{F}(4)$ with $0 \leq \Re\tau \leq 1$:

1. $\Re f(\tau) = 0$ if and only if τ lies on the semicircle $|2\tau - 1| = 1$ which separates the interiors of $\mathcal{F}^{\pm}(4)$.

2. $\Re f(\tau) > 0$ for at least one $\tau \in \mathcal{F}^+(4)$.

For the first fact implies that $\Re f(\tau)$ has constant nonzero sign on the two interiors. Since $f(\gamma\tau) = -f(\tau)$ for $\gamma \in \Gamma_0(2) \setminus \Gamma_0(4)$, the signs are different in the two interiors; and the second fact establishes that $\Re f(\tau)$ is positive in the interior of $\mathcal{F}^+(4)$.

Let $f = f(\tau)$. Let the roots of $X(X^2 + fX + 1)$ be $e_1 = 0, e_2, e_3$. Since $e_2 e_3 = 1$, we have $\Re f = 0$ if and only if $\Re e_2 = \Re e_3 = 0$ with the imaginary parts $\Im e_2$, $\Im e_3$ of opposite sign; so e_1, e_2, e_3 collinear, with 0 in between the other two roots. Conversely, if the e_j are colinear with 0 in the middle then (since $e_2 e_3 = 1$) it follows that $\Re f = 0$. However, this alignment of the roots happens precisely when the period lattice Λ_0 is rectangular, with orthogonal basis $w_2, w_1 + w_2$, which is when τ lies on the semicircle as claimed. This establishes the first fact.

Finally, one can check that for $i \in \mathcal{F}^+(4)$ we have $f(i) = 3/\sqrt{2} > 0$ (equivalently, $\lambda(2i) = (3 - 2\sqrt{2})/(3 + 2\sqrt{2})$ so that $|\lambda(2i)| < 1$). □

5 Chains of 2-Isogenies

From now on we will use standard Weierstrass models of elliptic curves rather than the special forms $E_{\{a,b\}}$ used above. Thus, let E_0 be an elliptic curve over $\mathbb{C}$ given by a Weierstrass equation

$$E_0 : \quad Y_0^2 = 4(X_0 - e_1^{(0)})(X_0 - e_2^{(0)})(X_0 - e_3^{(0)}), \tag{4}$$

where the roots $e_j^{(0)}$ are distinct, and $\sum_{j=1}^{3} e_j^{(0)} = 0$. We consider the ordering of the roots $e_j^{(0)}$ as fixed, with the point $T_0 = (e_1^{(0)}, 0)$ of order 2 as distinguished. Let

$$a_0 = \pm\sqrt{e_1^{(0)} - e_3^{(0)}}, \quad b_0 = \pm\sqrt{e_1^{(0)} - e_2^{(0)}};$$

the choice of signs will be discussed below. Via a shift of the X-coordinate we have $E_0 \cong E_{\{a_0,b_0\}}$, and the choice of signs determines the point $P_0 = (e_1^{(0)} + a_0 b_0, 2a_0 b_0(a_0 + b_0))$ of order 4 such that $2P_0 = T_0$.

Now consider arbitrary AGM sequences $((a_n, b_n))_{n=0}^{\infty}$ starting from (a_0, b_0). As in [2], for $n \geq 1$ we let

$$e_1^{(n)} = \frac{a_n^2 + b_n^2}{3}, \quad e_2^{(n)} = \frac{a_n^2 - 2b_n^2}{3}, \quad e_3^{(n)} = \frac{b_n^2 - 2a_n^2}{3}. \tag{5}$$

These equalities also hold for $n = 0$, and for all $n \geq 0$ the $e_j^{(n)}$ are distinct, and satisfy $\sum_{j=1}^{3} e_j^{(n)} = 0$. Hence each AGM sequence determines a sequence $(E_n)_{n=0}^{\infty}$ of elliptic curves defined over $\mathbb{C}$, where E_n is given by the Weierstrass equation

$$E_n : \quad Y_n^2 = 4(X_n - e_1^{(n)})(X_n - e_2^{(n)})(X_n - e_3^{(n)}). \tag{6}$$

Each has a distinguished 2-torsion point $T_n = (e_1^{(n)}, 0)$.

For $n \geq 1$, define a 2-isogeny $\varphi_n : E_n \to E_{n-1}$ via $(x_n, y_n) \mapsto (x_{n-1}, y_{n-1})$, where

$$
\begin{aligned}
x_{n-1} &= x_n + \frac{(e_3^{(n)} - e_1^{(n)})(e_3^{(n)} - e_2^{(n)})}{x_n - e_3^{(n)}}, \\
y_{n-1} &= y_n \left(1 - \frac{(e_3^{(n)} - e_1^{(n)})(e_3^{(n)} - e_2^{(n)})}{(x_n - e_3^{(n)})^2} \right).
\end{aligned} \tag{7}
$$

Now $\ker(\varphi_n) = \langle (e_3^{(n)}, 0) \rangle$, and

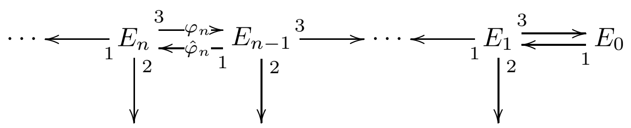
$$\varphi_n(T_n) = T_{n-1} = \varphi_n((e_2^{(n)}, 0)).$$

The dual isogeny $\hat{\varphi}_n : E_{n-1} \to E_n$ has kernel $\langle T_{n-1} \rangle \neq \ker(\varphi_{n-1})$, so is distinct from φ_{n-1}. Each composite $\varphi_n \circ \varphi_{n+1}$ has cyclic kernel, since

$$\varphi_n \left(\varphi_{n+1} \left(T_{n+1} \right) \right) = \varphi_n(T_n) = T_{n-1} \neq O.$$

Similarly, by tracing the images of T_n, we see that all composites of the φ_n have cyclic kernels.

This *chain of* 2*-isogenies* may be depicted thus:



The number j next to each arrow originating from E_n denotes the point $(e_j^{(n)}, 0)$ which generates the kernel of an associated 2-isogeny.

The construction of this isogeny chain from the original curve $E^{(0)}$ depends on many choices. The definition of a_0, b_0 depends first on which root is labelled $e_1^{(0)}$ (which determines T_0 and hence E_1), and the order of labelling of $e_2^{(0)}$ and $e_3^{(0)}$. Secondly, the signs for a_0, b_0 were arbitrary; changing just one of them changes P_0 and hence E_2. So, as in the previous section, the unordered pair $\{a_0, b_0\}$ determines the short isogeny chain $E_2 \to E_1 \to E_0$, with $\{-a_0, -b_0\}$ determining the same short chain. Finally, for each a_0, b_0, there are many AGM sequences, which determine the rest of the chain.

Note that we can rewrite $e_j^{(n+1)}$ given by (5) as

$$e_1^{(n+1)} = \frac{e_1^{(n)} + 2a_n b_n}{4}, \quad e_2^{(n+1)} = \frac{e_1^{(n)} - 2a_n b_n}{4}, \quad e_3^{(n+1)} = \frac{-e_1^{(n)}}{2}.$$

If (a_n, b_n) is replaced by $(a_n, -b_n)$ for $n \geq 1$, we see that this interchanges $e_1^{(n+1)}$ and $e_2^{(n+1)}$ but leaves $e_3^{(n+1)}$ unchanged. This does not change the curve E_{n+1}; it only changes the labelling of its roots, which then changes E_{n+2}.

Hence we have established a bijection between

- The set of all AGM sequences starting at (a_0, b_0), and
- The set of all isogeny chains starting with the short chain $E_2 \to E_1 \to E_0$.

We now consider what happens when $n \to \infty$. From (5), we have

$$\lim_{n\to\infty} e_1^{(n)} = \frac{2M^2}{3}, \quad \lim_{n\to\infty} e_2^{(n)} = \lim_{n\to\infty} e_3^{(n)} = \frac{-M^2}{3}, \tag{8}$$

where $M = M_S(a_0, b_0)$ for some set $S \subseteq \mathbb{Z}_{>0}$. The "limiting curve" E_∞ for the sequence $(E_n)_{n=0}^{\infty}$ is the singular curve

$$E_\infty : \quad Y_\infty^2 = 4\left(X_\infty - \frac{2}{3}M^2\right)\left(X_\infty + \frac{1}{3}M^2\right)^2. \tag{9}$$

Proposition 1 implies the following.

Proposition 13. *The singular point of E_∞ is a node if and only if the AGM sequence (a_n, b_n) is good.*

5.1 The associated lattice chain

For each $n \geq 0$, we have $E_n(\mathbb{C}) \cong \mathbb{C}/\Lambda_n$, where Λ_n is the lattice of periods of the differential dX_n/Y_n. From the definition of φ_n (see (7)), it can be verified that each φ_n is *normalised*, in the sense that

$$\varphi_n^* \left(\frac{dX_{n-1}}{Y_{n-1}}\right) = \frac{dX_n}{Y_n} \tag{10}$$

for all $n \geq 1$. Hence φ_n corresponds to the map $\mathbb{C}/\Lambda_n \to \mathbb{C}/\Lambda_{n-1}$ induced from the identity map $\mathbb{C} \to \mathbb{C}$. Since each φ_n is a 2-isogeny and the composites of the φ_n have cyclic kernels, it is clear that (Λ_n) is a lattice chain in the sense of Section 3.

This establishes the commutativity of the diagram (Figure 1), which shows the relationship between chains of lattices and chains of 2-isogenies. For brevity we denote $z \mapsto (\wp_\Lambda(z), \wp'_\Lambda(z))$ by $z \mapsto \wp_n(z)$.

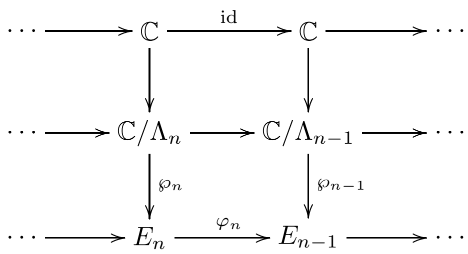


Figure 1: A chain of isogenies linked with a chain of lattices

Conversely, given any lattice chain (Λ_n) starting from Λ_0, we may recover the sequence of curves E_n and the chain of 2-isogenies linking them: first, Λ_1 determines which root of E_0 is labelled $e_1^{(0)}$; then Λ_2 determines the choice of signs in the definition of a_0, b_0; and finally the AGM sequence starting with (a_0, b_0) is determined by the Λ_n for $n \geq 2$.

Thus we have a third set in bijection with both the set of all AGM sequences starting at (a_0, b_0), and the set of all isogeny chains starting with the short chain $E_2 \to E_1 \to E_0$: namely, the set of all lattice chains starting with the short chain $\Lambda_0 \supset \Lambda_1 \supset \Lambda_2$.

Proposition 14. *With the above notation, for all $n \geq 0$,*

1. $E_n \cong E_{\{a_n,b_n\}}$;
2. $\Lambda_n \supset \Lambda_{n+1} \supset \Lambda_{n+2}$ *is a short chain in the sense of Section 3;*
3. Λ_{n+2} *is the right choice of sublattice of* Λ_{n+1} *if and only if* (a_n, b_n) *is a good pair;*
4. *the lattice chain* (Λ_n) *is good (respectively, optimal) if and only if the sequence* $((a_n, b_n))$ *is good (respectively, optimal).*

Proof. For (1), replace x_n by $x_n + e_1^{(n)}$ in the equation for E_n to obtain the equation for $E_{\{a_n,b_n\}}$. The rest is then is clear, using Theorem 10. □

6 Period Lattices of Elliptic Curves

6.1 General Case

Let E_0 be an elliptic curve over $\mathbb{C}$ of the form (4). We keep the notation of the preceding section; in particular, the period lattice of E_0 is Λ_0. Each primitive period $w_1 \in \Lambda_0$ determines a good lattice chain (Λ_n) where $\Lambda_n = \langle w_1 \rangle + 2^n\Lambda_0$, and conversely, since $\cap_n \Lambda_n = \langle w_1 \rangle$. So we have a bijection between the set of primitive periods of Λ_0 (up to sign) and good lattice chains. Each good lattice chain in turn determines a good AGM sequence $((a_n, b_n))$ starting at a pair (a_0, b_0) such that $E_0 \cong E_{\{a_0,b_0\}}$.

We now show that the period w_1 may be expressed simply in terms of the limit of the associated AGM sequence. It will follow that every primitive period w_1 of E_0 may be obtained from the limit of an appropriately chosen good AGM sequence. Conversely, we may express the set of all limits of AGM sequences starting at (a_0, b_0) in terms of periods of E_0. We will also show that optimal AGM sequences give periods which are minimal in their coset modulo $4\Lambda_0$, and super-optimal sequences (where the initial pair (a_0, b_0) also good) give periods which are minimal modulo $2\Lambda_0$. By Lemma 6, we will be then able to express a $\mathbb{Z}$-basis for Λ_0 in terms of specific AGM values.

Proposition 15. *Let* (Λ_n) *be a good lattice sequence with limiting period* w_1 *(generating* $\cap\Lambda_n$*, and defined up to sign). Then for all* $z \in \mathbb{C} \setminus \Lambda_0$ *we have*

$$\lim_{n\to\infty} \wp_{\Lambda_n}(z) = \left(\frac{\pi}{w_1}\right)^2 \left(\frac{1}{\sin^2(z\pi/w_1)} - \frac{1}{3}\right)$$
$$\lim_{n\to\infty} \wp'_{\Lambda_n}(z) = -2\left(\frac{\pi}{w_1}\right)^3 \left(\frac{\cos(z\pi/w_1)}{\sin^3(z\pi/w_1)}\right).$$

Proof. Since w_1 is primitive, there exists $w_2 \in \mathbb{C}$ such that $\Lambda_n = \langle w_1, 2^n w_2 \rangle$ for all $n \geq 0$. In the standard series expansion

$$\wp_{\Lambda_n}(z) = \frac{1}{z^2} + \sum_{0\neq w\in\Lambda_n} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2}\right),$$

we set $w = m_1 w_1 + m_2 2^n w_2$ with m_1, m_2 not both zero. As $n \to \infty$ all terms with $m_2 \neq 0$ tend to zero, leaving

$$\lim_{n\to\infty} \wp_{\Lambda_n}(z) = \sum_{m\in\mathbb{Z}} \frac{1}{(z - mw_1)^2} - \frac{1}{3}\left(\frac{\pi}{w_1}\right)^2.$$

Using the expansion $\pi^2/\sin^2(\pi z) = \sum_{m\in\mathbb{Z}} 1/(z-m)^2$, this simplifies to the formula given.

For $\lim_{n\to\infty} \wp'_{\Lambda_n}(z)$, we may either differentiate this, or apply the same argument to the series expansion of $\wp'_{\Lambda_n}(z)$. □

Corollary 16. *In the above notation, let (Λ_n) be a (good) lattice chain, with limiting period w_1, associated to the elliptic curve E_0 and the (good) AGM sequence $((a_n, b_n))$ with non-zero limit $M = M_S(a_0, b_0)$. Then $M = \pm\pi/w_1$, so that the period w_1 may be determined up to sign by*

$$w_1 = \pm\pi/M_S(a_0, b_0).$$

Proof. For all $n \geq 0$ we have $\wp_{\Lambda_n}(w_1/2) = e_1^{(n)}$. Letting $n \to \infty$ and using the proposition we find that

$$\frac{2}{3}M^2 = \lim_{n\to\infty} e_1^{(n)} = \frac{2}{3}\left(\frac{\pi}{w_1}\right)^2,$$

from which the result follows. □

The ambiguity of sign in this result will not matter in practice: changing the sign of w_1 does not change the lattice chain, and neither does changing the signs of both a_0, b_0 (and hence the sign of $M_S(a_0, b_0)$).

For fixed (a_0, b_0), the value of $M_S(a_0, b_0)$ depends on the set S of indices n for which (a_n, b_n) is bad. Changing S, we obtain different AGM sequences, and different lattice chains, but these all start with the same short chain $(\Lambda_n)_{n=0}^2$, and the periods given by $\pi/M_S(a_0, b_0)$ are all in the same coset modulo $4\Lambda_0$. We may now establish the result stated above as Proposition 1(3):

Corollary 17. *$|M_S(a_0, b_0)|$ attains its maximum (among all AGM-sequences starting at (a_0, b_0)) if and only if the sequence is optimal.*

Proof. By Corollary 16, $M_S(a_0, b_0)$ is maximal (in absolute value) if and only if the limiting period $w_1 = \pi/M_S(a_0, b_0)$ is minimal. By Proposition 7, this is if and only if the lattice chain is optimal. By Proposition 14(4), this in turn is if and only if the AGM sequence is optimal. □

Corollary 18. *1. The optimal value $M = M(a_0, b_0)$ gives a period $w_1 = \pi/M$ which is minimal in its coset modulo $4\Lambda_0$.*

2. $|M(a_0, b_0)| \geq |M(a_0, -b_0)| \iff |a_0 - b_0| \leq |a_0 + b_0|$.

3. If (a_0, b_0) is good, then $\pi/M(a_0, b_0)$ is minimal in its coset modulo $2\Lambda_0$.

Proof. Changing the sign of b_0 (only) does not change Λ_1 (or E_1), but does change Λ_2. The effect on w_1, therefore, is to change its coset modulo $4\Lambda_0$ while not affecting its coset modulo $2\Lambda_0$. By Proposition 10, Λ_2 is the right choice if and only if (a_0, b_0) is good. Hence, to obtain a period minimal in its coset modulo $2\Lambda_0$, and not just modulo $4\Lambda_0$, we choose the sign of b_0 so that the pair (a_0, b_0) is good, and then take an optimal AGM sequence. ☐

Theorem 19 (Periods of Elliptic Curves over $\mathbb{C}$, first version)**.** *Let E be an elliptic curve over $\mathbb{C}$ given by the Weierstrass equation*

$$Y^2 = 4(X - e_1)(X - e_2)(X - e_3),$$

with period lattice Λ. Set $a_0 = \sqrt{e_1 - e_3}$ and $b_0 = \sqrt{e_1 - e_2}$, where the signs are chosen so that (a_0, b_0) is good, i.e., $|a_0 - b_0| \leq |a_0 + b_0|$, and let

$$w_1 = \frac{\pi}{M(a_0, b_0)},$$

using the optimal value of the AGM. Then w_1 is a primitive period of E, and is a minimal period in its coset modulo 2Λ.

Define w_2, w_3 similarly by permuting the e_j; then any two of w_1, w_2, w_3 form a $\mathbb{Z}$-basis for Λ.

Proof. Everything has been established except the last part. Letting e_2, e_3 in turn play the role of e_1 gives minimal periods in each of the cosets modulo 2Λ, so Lemma 6 applies. ☐

Algorithm 20 (Computation of a period lattice basis)**.**

Input: An elliptic curve E defined over $\mathbb{C}$, and roots $e_j \in \mathbb{C}$ for $j = 1, 2, 3$.

Output: Three primitive periods of E, which are minimal coset representatives, any two of which form a $\mathbb{Z}$-basis for the period lattice of E.

1. Label one of the roots as e_1, and the other two arbitrarily as e_2, e_3;
2. Set $a_0 = \sqrt{e_1 - e_3}$ with arbitrary sign, and then $b_0 = \pm\sqrt{e_1 - e_2}$ with the sign chosen such that $|a_0 - b_0| \leq |a_0 + b_0|$.
3. Output $w = \pi/M(a_0, b_0)$, using the optimal value of the AGM.
4. Repeat with each root e_j in turn playing the role of e_1.

Instead of computing w_2, w_3 by permuting the e_j as in Theorem 19, we may alternatively obtain all w_j by using a single ordering of the roots and three different AGM computations.

Starting with an arbitrary ordering of the roots,say (e_1, e_2, e_3), define a and b as before, up to sign, by $a^2 = e_1 - e_3$ and $b^2 = e_1 - e_2$; and also define c (up to sign) by $c^2 = e_2 - e_3$, so that $a^2 = b^2 + c^2$. We would like to determine the signs of a, b, c so that all three of the following conditions hold:

$$|a - b| \leq |a + b|, \quad |c - ib| \leq |c + ib|, \quad |a - c| \leq |a + c|. \qquad (11)$$

We claim that this is always possible. To see this, first choose the sign of a arbitrarily. Then choose the signs of b and c so that the first and the third conditions in (11) hold. Finally, if the second condition fails, one can easily check that if e_1 and e_3 are interchanged and a, b, c replaced (in order) by ia, ic, ib, then all three inequalities will hold.

We can now state an alternative theorem for obtaining a $\mathbb{Z}$-basis for the period lattice Λ of E.

Theorem 21 (Periods of Elliptic Curves over $\mathbb{C}$, second version)**.** *Let E be an elliptic curve over $\mathbb{C}$ given by the Weierstrass equation*

$$Y^2 = 4(X - e_1)(X - e_2)(X - e_3),$$

with period lattice Λ. Order the roots (e_1, e_2, e_3) of E, so that the signs of $a = \sqrt{e_1 - e_3}$, $b = \sqrt{e_1 - e_2}$, $c = \sqrt{e_2 - e_3}$ may be chosen to satisfy all the conditions of (11)*. Define*

$$w_1 = \frac{\pi}{M(a, b)}, \quad w_2 = \frac{\pi}{M(c, ib)}, \quad w_3 = \frac{i\pi}{M(a, c)}.$$

Then each w_j is a primitive period, minimal in its coset modulo 2Λ, and any two of the w_j form a $\mathbb{Z}$-basis for Λ.

Proof. Let (e_1, e_2, e_3) be an order of the roots of E_0. Interchanging e_1 and e_3 if necessary, define $a = \sqrt{e_1 - e_3}$, $b = \sqrt{e_1 - e_2}$, $c = \sqrt{e_2 - e_3}$, with the signs chosen so that all three inequalities in (11) hold.

Now $w_1 = \pi/M(a, b)$ is primitive and minimal in its coset as before, since (a, b) is good. Using $(e'_1, e'_2, e'_3) = (e_2, e_1, e_3)$, we find that $(a', b') = (c, ib)$ is good, and set $w_2 = \pi/M(a', b') = \pi/M(c, ib)$; and using $(e''_1, e''_2, e''_3) = (e_3, e_2, e_1)$, we see that $(a'', b'') = (ia, ic)$ is good, and set $w_3 = \pi/M(a'', b'') = \pi i/M(a, c)$. □

We complete this section by considering two special cases, which arise when considering elliptic curves defined over the real numbers, separating the cases of positive discriminant (rectangular period lattice) and negative discriminant.

6.2 Special Case I: Rectangular Lattices

For the rest of this section, we set $i = \sqrt{-1}$. Recall that if $|a_0 - b_0| = |a_0 + b_0|$, then both $(a_0, \pm b_0)$ are good and $\Re(b_0/a_0) = 0$. Then

$$\frac{e_2 - e_1}{e_3 - e_1} = (b_0/a_0)^2$$

is real and negative. Geometrically, this means that the e_j are collinear on the complex plane with e_1 in the middle.

To see what the associated period lattice looks like, let $w = \pi/M(a_0, b_0)$ and $w' = \pi/M(a_0, -b_0)$. Then w, w' are both minimal elements in the same coset modulo $2\Lambda_0$. By Lemma 5, the periods $w_1, w_2 = (w \pm w')/2$ form an orthogonal $\mathbb{Z}$-basis for Λ_0, and the period lattice is rectangular. Alternatively, we could obtain a $\mathbb{Z}$-basis for Λ_0 by computing two periods (as in Theorem 19) using the two other roots of E which are not "in the middle" in the role of e_1.

Finally, we note that whenever the e_j are collinear, we can "rotate" them by a multiplying by a suitable constant in $\mathbb{C}^*$ so that the scaled roots e'_j are all real. Then one could use an algorithm for computing period lattices of elliptic curves over $\mathbb{R}$ (e.g. [3, Algorithm 7.4.7]) to compute the period lattice of the elliptic curve $(Y')^2 = 4(X' - e_1')(X' - e_2')(X' - e_3')$. The period lattice of our original elliptic curve is then obtained after suitable scaling. This may be more efficient in practice, since only real arithmetic would be needed in the AGM iteration.

If the e_j are all real (as is the case for an elliptic curve defined over $\mathbb{R}$ with positive discriminant), we may order them so that $e_1 > e_2 > e_3$ and obtain a rectangular basis for the period lattice by setting

$$w_1 = \pi/M(\sqrt{e_1 - e_2}, \sqrt{e_1 - e_3}), \quad w_2 = \pi i/M(\sqrt{e_2 - e_3}, \sqrt{e_1 - e_3}) \qquad (12)$$

with all square roots positive; then w_1 and w_2/i are both real and positive. These familiar formulas may be found in [3, Algorithm 7.4.7] or [5, (3.7.1)].

6.3 Special Case II

If the roots of E are such that

$$\left|\frac{e_1 - e_2}{e_1 - e_3}\right| = 1 \quad \text{with } e_1 - e_2 \neq \pm(e_1 - e_3),$$

then geometrically the e_j lie on an isosceles triangle having e_1 as the vertex where the sides of equal length intersect. As before, one can rotate this triangle by a suitable constant in $\mathbb{C}^*$ so that $e_1 \in \mathbb{R}$, and e_2, e_3 are complex conjugates. This yields a new elliptic curve E', defined over $\mathbb{R}$, whose Weierstrass equation has only one real root.

Again, one could use an algorithm for computing period lattices of elliptic curves over $\mathbb{R}$ (e.g. [3, Algorithm 7.4.7]) to compute the period lattice of E'. This is of the form $\Lambda' = \langle w_1', w_2' \rangle$, for some w_1', w_2' satisfying

$$w_1' \in \mathbb{R}, \quad \Re(w_2') = \frac{w_1'}{2}.$$

The period lattice $\Lambda = \langle w_1, w_2 \rangle$ of E, with $\Re(w_2/w_1) = 1/2$, can then be obtained by a suitable scaling of w_1', w_2'. This will be illustrated in Example 4.

For real curves with negative discriminant, we present here a simplification of the purely real algorithm given in [3]. Let e_1 be real and e_2, e_3 complex conjugates, ordered so that $\Im e_2 > 0$. Set $a_0 = \sqrt{e_1 - e_3} = x + yi$; since $e_1 - e_3$ lies in the upper half-plane, we may choose the sign of a_0 so that $x, y > 0$. Set $r = \sqrt{x^2 + y^2} > 0$ and $b_0 = \sqrt{e_1 - e_2} = x - yi$. Now we may obtain a real period w_+ from

$$w_+ = \pi/M(a_0, b_0) = \pi/M(x + yi, x - yi) = \pi/M(x, r),$$

and an imaginary period w_- from

$$w_- = \pi/M(-a_0, b_0) = \pi i/M(y - xi, y + xi) = \pi i/M(y, r).$$

Note that both AGMs appearing here, $M(x, r)$ and $M(y, r)$, are classical (real and positive). These periods span a sublattice of index 2 in the period lattice, for which a $\mathbb{Z}$-basis may be taken to be $w_1 = w_+$ and $w_2 = (w_+ + w_-)/2$, where $\Re(w_2/w_1) = 1/2$.

7 The complete set of AGM values

In 1800, Gauss described the complete set of values of $M_S(a,b)$ as S ranges through all finite sets. The proof given by Cox in [4, Theorem 2.2] uses theta and modular functions related to the modular functions which appeared earlier in this paper. Other proofs are also available in the literature, for example by Geppert [7].

We will give here a slightly more general form of the result than that stated in [4], and give an alternative proof which brings out clearly the relation with period lattices of elliptic curves.

In the following statement, we set $P_S(a,b) = \pi/M_S(a,b)$ (for any finite $S \subseteq \mathbb{Z}_{>0}$) and $P(a,b) = \pi/M(a,b)$.

Theorem 22. *For $a,b \in \mathbb{C}^*$ with $a \neq \pm b$, let $E_{\{a,b\}}$ be the elliptic curve over $\mathbb{C}$ given by the Weierstrass equation*

$$E_{\{a,b\}}: \quad Y^2 = 4X(X+a^2)(X+b^2),$$

and let Λ be its period lattice. Let $c = \sqrt{a^2-b^2}$, with the sign chosen so that the pair (a,c) is good, and set

$$w_1 = P(a,b), \quad w_3 = iP(a,c).$$

Then $\Lambda = \mathbb{Z}w_1 + \mathbb{Z}w_3$, and the set of values of $P_S(a,b)$ is precisely the set of primitive elements of the coset $w_1 + 4\Lambda$. More precisely, we have the following:

$$\begin{aligned}
\{P_S(a,b)\} &= \{w \in w_1 + 4\Lambda, \quad w \text{ primitive}\};\\
\{P_S(a,-b)\} &= \{w \in w_1 + 2w_3 + 4\Lambda, \quad w \text{ primitive}\};\\
\{P_S(-a,-b)\} &= \{w \in -w_1 + 4\Lambda, \quad w \text{ primitive}\};\\
\{P_S(-a,b)\} &= \{w \in -w_1 + 2w_3 + 4\Lambda, \quad w \text{ primitive}\}.
\end{aligned}$$

Thus, the complete set of all values of $P_S(\pm a, \pm b)$ is the set of primitive elements of the coset $w_1 + 2\Lambda$.

Proof. Since Λ is invariant under translations of the X-coordinate, we may apply Theorem 21 to see that $\Lambda = \mathbb{Z}w_1' + \mathbb{Z}w_3$ where w_3 (as given) is a minimal coset representative, and either

- (a,b) is good and $w_1' = w_1$; or
- (a,b) is bad and $w_1' = w_1 \pm 2w_3$.

In either case, $\Lambda = \mathbb{Z}w_1 + \mathbb{Z}w_3$.

Now the values of $P_S(a,b)$ are precisely the primitive periods in the same coset as $w_1 = P(a,b)$ modulo 4Λ. Secondly, $P_S(-a,-b) = -P_S(a,b) = -w_1$, so the values of $P_S(-a,-b)$ are the primitive periods in the coset $-w_1 \pmod{4\Lambda}$, as required. Next, $P(a,-b)$ is the minimal period in the coset $w_1 + 2w_3 + 4\Lambda$, since this is the other coset modulo 4Λ contained in $w_1 + 2\Lambda$, so the values of $\pm P_S(a,-b)$ are also as stated. ☐

Corollary 23. *Let $a,b,c \in \mathbb{C}^*$ satisfy $a^2 = b^2 + c^2$. Define $w = \pi/M(a,b)$ and $w' = \pi i/M(a,c)$, where (a,c) is a good pair. Then*

1. $\Lambda = \mathbb{Z}w + \mathbb{Z}w'$ *is a lattice in* $\mathbb{C}$*;*

2. *the set of values of* $\pi/M_S(a,b)$ *is the set of primitive elements of the coset* $w + 4\Lambda$*; that is, the set*

$$\{uw + vw' \mid u,v \in \mathbb{Z},\ \gcd(u,v) = 1,\ u - 1 \equiv v \equiv 0 \pmod 4\};$$

3. *the set of values of* $\pi/M_S(\pm a, \pm b)$ *is the set of primitive elements of the coset* $w + 2\Lambda$*; that is, the set*

$$\{uw + vw' \mid u,v \in \mathbb{Z},\ \gcd(u,v) = 1,\ u - 1 \equiv v \equiv 0 \pmod 2\}.$$

8 Elliptic Logarithms

We now extend the method for computing periods of elliptic curves in Section 6 to give a method for computing elliptic logarithms of points on elliptic curves.

Let E be an elliptic curve over $\mathbb{C}$ given by a Weierstrass equation as before, and Λ the lattice of periods of the differential dX/Y on E, so that $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$. An *elliptic logarithm* of $P \in E(\mathbb{C})$ is a value $z_P \in \mathbb{C}$ such that $P = (\wp_\Lambda(z_P), \wp'_\Lambda(z_P))$. Note that z_P is only well-defined modulo Λ. We wish to have an algorithm which can compute the numerical value of the complex number z_P, to any required precision, from the coefficients of E and the coordinates of P (which we assume are given exactly, or are available to arbitrary precision).

Construct as before an isogeny chain (E_n) with $E_0 = E$, with associated lattice chain (Λ_n) (with $\Lambda_0 = \Lambda$) and AGM sequence (a_n, b_n). We will assume that the chain is super-optimal with $|a_n - b_n| < |a_n + b_n|$ for all $n \geq 0$. (This is possible except when Λ_0 is rectangular, and even then is possible for two of the three super-optimal sequences). Let w_1, w_2 be a $\mathbb{Z}$-basis for Λ such that $\Lambda_n = \langle w_1, 2^n w_2 \rangle$ for all $n \geq 0$. We have 2-isogenies $\varphi_n : E_n \to E_{n-1}$ for $n \geq 1$, induced by the natural maps $\mathbb{C}/\Lambda_n \to \mathbb{C}/\Lambda_{n-1}$.

8.1 Coherent point sequences

Consider sequences of points $(P_n)_{n=0}^{\infty}$ where $P_n \in E_n(\mathbb{C})$ satisfy $\varphi_n(P_n) = P_{n-1}$ for all $n \geq 1$. Such a sequence will be called *coherent* if there exists $z \in \mathbb{C}$ such that $P_n = \wp_n(z)$ for all $n \geq 0$; here, as above, we write $\wp_n(z)$ for $(\wp_{\Lambda_n}(z), \wp'_{\Lambda_n}(z))$. If such a z exists, it is uniquely determined modulo $\cap\Lambda_n = \Lambda_\infty = \langle w_1 \rangle$.

In general there are uncountably many point sequences with a fixed starting point P_0, since for each $P_n \in E_n(\mathbb{C})$ there are two points $P_{n+1} \in E_{n+1}(\mathbb{C})$ with $\varphi_{n+1}(P_{n+1}) = P_n$. However, only countably many of these are coherent, since $\wp_0^{-1}(P_0)$ is a coset of Λ_0 in $\mathbb{C}$, and hence countable.

For example, taking $z = 0$ shows that the trivial sequence (O_n), where O_n is the base point on E_n, is coherent. Also, the sequence with $P_n = T_n = (e_1^{(n)}, 0)$ is coherent, via $z = w_1/2$.

Given a point sequence (P_n), for each n let $C_n = \wp_n^{-1}(P_n) \subset \mathbb{C}$ be the complete set of all the elliptic logarithms of P_n, which is a coset of Λ_n in $\mathbb{C}$. Since Λ_{n+1} has index 2 in Λ_n, each C_n is the disjoint union of two cosets of Λ_{n+1}, one of these being C_{n+1}; the other is the set of elliptic logarithms of the second point $P'_{n+1} \in E_{n+1}(\mathbb{C})$ such that $\varphi_{n+1}(P'_{n+1}) = P_n$. Thus we have

$$C_0 \supset C_1 \supset \cdots \supset C_n \supset C_{n+1} \supset \dots.$$

The point sequence is coherent if and only if $C_\infty = \cap_{n=0}^\infty C_n \neq \emptyset$, in which case C_∞ is a coset of Λ_∞ in $\mathbb{C}$.

An argument similar to that used above for Lemma 3 shows the following.

Lemma 24. *The sequence (P_n) is coherent if and only if C_{n+1} contains the smallest element of C_n for almost all $n \geq 0$.*

8.2 The elliptic logarithm formula

Proposition 25. *With notation as above, let (P_n) be a coherent point sequence determined by $z \in \mathbb{C}$. Assume that $2z \notin \Lambda_\infty$. Then for n sufficiently large, we have $P_n \neq O_n$, and write $P_n = (x_n, y_n)$. Let $P_\infty = (x_\infty, y_\infty) \in E_\infty(\mathbb{C})$ be the limit point, defined by $(x_\infty, y_\infty) = \lim_{n\to\infty}(x_n, y_n)$. Set $M = \pi/w_1$, and*

$$t_\infty = -\frac{1}{2} y_\infty/(x_\infty + M^2/3).$$

Then $t_\infty \neq 0, \infty$, and (modulo Λ_∞) we have

$$z = \frac{1}{M}\arctan\left(\frac{M}{t_\infty}\right) = \frac{w_1}{\pi}\arctan\left(\frac{\pi}{w_1 t_\infty}\right). \tag{13}$$

Proof. Since $z \notin \Lambda_\infty$, for all $n \gg 0$ we have $z \notin \Lambda_n$, so that $P_n \neq O_n$. Proposition 15 gives expressions for the coordinates of $P_\infty = (x_\infty, y_\infty) \in E_\infty(\mathbb{C})$ in terms of M, $s = \sin(z\pi/w_1)$ and $c = \cos(z\pi/w_1)$:

$$x_\infty = M^2\left(\frac{1}{s^2} - \frac{1}{3}\right); \qquad y_\infty = -2M^3\frac{c}{s^3}.$$

Note that $s \neq 0$, since $z \notin \Lambda_\infty$; also, $s \neq \pm 1$ (and $c \neq 0$) since $2z \notin \Lambda_\infty$. Thus $x_\infty + M^2/3 = M^2/s^2 \neq 0$, and $t_\infty = -\frac{1}{2}y_\infty/(x_\infty + M^2/3) = Mc/s \neq 0$, giving formula (13). Taking different values of the multiple-valued function arctan changes z by integer multiples of w_1; so this formula gives a well defined value for z modulo Λ_∞, as desired. □

This result does also apply when $z = \pm w_1/2 \pmod{\Lambda_\infty}$, for then $s = \pm 1$ and $c = 0$, so $x_\infty + M^2/3 = M^2$ and $y_\infty = 0$, giving $t_\infty = 0$ and $z = w_1$; this is the case we used above to compute periods.

Proposition 25, and in particular formula (13), is the key to our elliptic logarithm algorithm, in which we will compute a sequence (t_n) iteratively such that $\lim t_n = t_\infty$. However, we derived (12) by starting from a value of $z \in \mathbb{C}$, rather than from the coordinates of a point $P = \wp(z) \in E(\mathbb{C})$. In order to produce an algorithm for computing z from the coordinates of P, we must show how to construct inductively a suitable coherent sequence of points, so that the limits x_∞, y_∞ and t_∞ exist. We will do this in the next subsection.

Remark. Our formula (13) is similar to the one used in Cohen's algorithm [3, Algorithm 7.4.8] for computing elliptic logarithms of real points on elliptic curves defined over $\mathbb{R}$. The variable denoted c_n in [3] is related to our t_n (defined below) by $c_n^2 = t_n^2 + a_n^2$; setting $c_\infty = \lim_{n\to\infty} c_n$, so that $c_\infty^2 = t_\infty^2 + M^2$, we can rewrite z_P as

$$z_P = \pm\frac{1}{M}\arcsin\left(\frac{M}{c_\infty}\right),$$

which is similar (up to sign) to the output of Cohen's algorithm. This approach leaves an ambiguity of the sign of z_P, which is resolved in [3] by considering the sign of y_0 at the end, something which is only possible in the real case. Using t_∞ instead of c_∞ avoids the ambiguity.

8.3 The elliptic logarithm iteration

Let $P = (x, y) \in E(\mathbb{C})$, where as above E is the elliptic curve with equation

$$E: \qquad Y^2 = 4(X - e_1)(X - e_2)(X - e_3).$$

In order to compute the elliptic logarithm z_P of P using (13), we need to find a suitable coherent point sequence (P_n) starting at $P_0 = P$. We iteratively compute P_1, P_2, ..., using the explicit formulas for the isogenies φ_n; at each stage there are two possible choices for P_n, determined by choosing a specific sign for a square root. The main issue is how to make these choices in such a way that the sequences converge.

It is simpler in practice to use alternative models for the elliptic curves in the sequence, in which the isogeny formulas are simpler. We introduce these now. Let E_1' be the curve with equation

$$E_1': \qquad R^2 = (T^2 + a^2)/(T^2 + b^2).$$

We regard E_1' as a projective curve in $\mathbb{P}^1 \times \mathbb{P}^1$, with points at infinity given by $(t, r) = (\infty, \pm 1), (\pm bi, \infty)$.

Define a map $\alpha : E_1' \to E$ by[2] $(t, r) \mapsto (x, y) = (t^2 + e_1, -2rt(t^2 + b^2))$, where as usual $a^2 = e_1 - e_3$ and $b^2 = e_1 - e_2$. This map is unramified and has degree 2; it sends $(\infty, \pm 1) \mapsto O_E$, $(\pm bi, \infty) \mapsto (e_2, 0)$, $(0, \pm a/b) \mapsto (e_1, 0)$ and $(\pm ai, 0) \mapsto (e_3, 0)$.

Write a_1, b_1 for the arithmetic and geometric means of a, b as usual, set

$$\begin{aligned} e_1' &= (a_1^2 + b_1^2)/3 = (a^2 + 6ab + b^2)/12, \\ e_2' &= (a_1^2 - 2b_1^2)/3 = (a^2 - 6ab + b^2)/12, \\ e_3' &= (b_1^2 - 2a_1^2)/3 = -(a^2 + b^2)/6, \end{aligned}$$

so that E_1 has with Weierstrass equation

$$E_1: \qquad Y_1^2 = 4(X_1 - e_1')(X_1 - e_2')(X_1 - e_3').$$

Now $E_1' \cong E_1$ via the isomorphism θ given by $(t, r) \mapsto (x_1, y_1)$ where

$$(x_1, y_1) = (\frac{1}{2}(t^2 + r(t^2 + a^2) + \frac{1}{6}(a^2 + b^2)), t(t^2 + r(t^2 + a^2) + \frac{1}{2}(a^2 + b^2)),$$

[2]The sign of y here is chosen to avoid a minus sign in the elliptic logarithm formula (13).

with inverse

$$(x_1, y_1) \mapsto (t, r) = \left(\frac{3y_1}{6x_1 + a^2 + b^2}, \frac{12x_1 + 5a^2 - b^2}{12x_1 + 5b^2 - a^2} \right).$$

The composite $\alpha \circ \theta^{-1} : E_1 \to E_1' \to E$ is the 2-isogeny denoted φ in Section 5.

Given a complete 2-isogeny chain $(E_n)_{n \geq 0}$ with $E_0 = E$, as in Section 5, we define for each $n \geq 1$ a curve E_n' with equation $R_n^2 = (T_n^2 + a_{n-1}^2)/(T_n^2 + b_{n-1}^2)$, isomorphic to E_n via θ_n (defined as for $\theta = \theta_1$ as above); these fit into a commutative diagram

$$\begin{array}{ccccccccc}
\cdots \longrightarrow & E_n' & \xrightarrow{\varphi_n'} & E_{n-1}' & \longrightarrow \cdots \longrightarrow & E_1' & & & \\
& \downarrow{\scriptstyle \theta_n} & & \downarrow{\scriptstyle \theta_{n-1}} & & \downarrow{\scriptstyle \theta_1} & \searrow^{\alpha} & & \\
\cdots \longrightarrow & E_n & \xrightarrow{\varphi_n} & E_{n-1} & \longrightarrow \cdots \longrightarrow & E_1 & \xrightarrow{\varphi_1} & E_0 &
\end{array}$$

where $\varphi_n' : E_n' \to E_{n-1}'$ is the 2-isogeny which makes the diagram commute. A little algebra shows that φ_n' is given by

$$r_{n-1} = \frac{t_n^2 + a_{n-1}a_{n-2}}{t_n^2 + a_{n-1}b_{n-2}} = \frac{a_{n-2}r_n^2 - a_{n-1}}{-b_{n-2}r_n^2 + a_{n-1}}, \qquad t_{n-1} = \frac{t_n}{r_n}.$$

For any point sequence (P_n) (with $P_n \in E_n(\mathbb{C})$ and $\varphi_{n+1}(P_{n+1}) = P_n$ for all $n \geq 0$) we set $P_n' = (r_n, t_n) = \theta_n^{-1}(P_n) \in E_n'(\mathbb{C})$ for $n \geq 1$. Since $\alpha(P_1') = P_0$, we have

$$r_1^2 = \frac{x_0 - e_3}{x_0 - e_2}, \qquad \text{and} \qquad t_1 = -\frac{y_0}{2r_1(x_0 - e_2)} = \sqrt{x_0 - e_1};$$

note that these equations determine r_1 (and then t_1) up to sign. Next, from $\varphi_n'(P_n') = P_{n-1}'$ for $n \geq 2$, we have

$$r_n^2 = \frac{a_{n-1}(r_{n-1} + 1)}{b_{n-2}r_{n-1} + a_{n-2}}, \qquad \text{and} \qquad t_n = r_n t_{n-1};$$

again, these determine (r_n, t_n) up to sign.

Hence we may construct all possible point sequences (P_n') with $P_n' \in E_n'(\mathbb{C})$ for $n \geq 1$, starting from $P_0 = (x_0, y_0) \in E_0(\mathbb{C})$ with $y_0 \neq 0$, by initialising

$$r_1 = \sqrt{\frac{x_0 - e_3}{x_0 - e_2}}, \qquad \text{and} \qquad t_1 = -\frac{y_0}{2r_1(x_0 - e_2)}$$

to determine $P_1' = (r_1, t_1)$, and then iterating the following to obtain $P_n' = (r_n, t_n)$ for $n \geq 2$:

$$r_n = \sqrt{\frac{a_{n-1}(r_{n-1} + 1)}{b_{n-2}r_{n-1} + a_{n-2}}}, \qquad \text{and} \qquad t_n = r_n t_{n-1}.$$

Suitable choices of signs of r_n will be discussed below, which will ensure that these sequences converge. Then we will have $r_\infty = \lim r_n = 1$ and $t_\infty = \lim t_n$ satisfying

$$x_\infty = t_\infty^2 + \frac{2}{3}M^2, \qquad y_\infty = -2t_\infty(t_\infty^2 + M^2),$$

where $M = \mathrm{AGM}(a, b)$ as usual. It follows that

$$t_\infty = \frac{-y_\infty/2}{x_\infty + M^2/3},$$

as in the statement of Proposition 25.

8.4 Choice of signs in the iteration

We now show that we do obtain coherent, convergent sequences, provided that for all (or all but finitely many) n we choose the sign of r_n so that $\Re(r_n) \geq 0$; always assuming that the isogeny sequence itself is optimal.

Proposition 26. *With the notation of the previous section, assume that the AGM sequence satisfies $\Re(a_n/b_n) > 0$ for all $n \geq 0$.*

If $\Re r_n \geq 0$ for all $n \geq 1$, then the point sequence $(P_n) = (\theta_n(r_n, t_n))$ determined by the iteratively defined sequence of pairs (r_n, t_n) is coherent.

The same conclusion holds if $\Re r_n \geq 0$ for all but finitely many $n \geq 1$.

Proof. Recall that Λ_n is the period lattice of E_n for $n \geq 0$, with $\mathbb{Z}$-basis w_1, w_2 such that $w_1 = \pi/M(a_0, b_0)$ generates $\cap_n \Lambda_n$, and $\Lambda_n = \langle w_1, 2^n w_2 \rangle$ for all $n \geq 0$. So for each n there exists $z_n \in \mathbb{C}$, uniquely determined modulo Λ_n, such that $x_n = \wp_{\Lambda_n}(z_n)$ and $y_n = \wp'_{\Lambda_n}(z_n)$. We wish to show that the z_n may be chosen independently of n.

Since

$$r_n = \frac{12x_n + 5a_{n-1}^2 - b_{n-1}^2}{12x_n + 5b_{n-1}^2 - a_{n-1}^2},$$

we may regard r_n as the value at z_n of an elliptic function f_n of degree 2 with respect to Λ_n. Similarly its square,

$$r_n^2 = \frac{x_{n-1} - e_3^{(n-1)}}{x_{n-1} - e_2^{(n-1)}},$$

is the value at z_n of f_n^2, which is an elliptic function with respect to the larger lattice Λ_{n-1}. It follows that

$$f_n(z + 2^{n-1}w_2) = -f_n(z)$$

for all $z \in \mathbb{C}$ and all $n \geq 1$.

Since

$$\wp_n(0) = O_E = \theta_n((\infty, 1))$$

and

$$\wp_n(w_1/2) = (e_1^{(n)}, 0) = \theta_n((0, a_{n-1}/b_{n-1})),$$

we have $f_n(0) = 1$ and $f_n(w_1/2) = a_{n-1}/b_{n-1}$ for all $n \geq 1$.

We now consider the preimage $\mathcal{R}_n$ of the right half-plane under f_n, for $n \geq 1$. Since $f_n(w_1/2) = a_{n-1}/b_{n-1}$ and $\Re(a_{n-1}/b_{n-1}) > 0$, this contains $w_1/2$ for all n. Let $\mathcal{R}_n^o$ denote the connected component of $\mathcal{R}_n$ which contains $w_1/2$. Both $\mathcal{R}_n$ and $\mathcal{R}_n^o$ are invariant under translation by w_1 (by periodicity of f_n), and $\mathcal{R}_n$ is the union of all translates of $\mathcal{R}_n^o$ by multiples of $2^n w_2$. The preimage of the left half-plane under f_n is $\mathcal{L}_n = \mathcal{R}_n + 2^{n-1}w_2$, which is the union of the translates of $\mathcal{R}_n^o$ by odd multiples of $2^{n-1}w_2$.

Consider a point $P_n = \wp_n(z_n) \in E_n(\mathbb{C})$, where $z_n \in \mathcal{R}_n^o$. Its preimages in $E_{n+1}(\mathbb{C})$ are $\wp_{n+1}(z_n)$ and $\wp_{n+1}(z_n')$, where $z_n' = z_n + 2^n w_2$. One of z_n, z_n' lies in $\mathcal{R}_{n+1}$, the other in $\mathcal{L}_{n+1}$. Since $w_1/2 \in \mathcal{R}_k^o$ for all k, one can show that $\mathcal{R}_n^o \subset \mathcal{R}_{n+1}^o$ (see Lemma 27 below). Hence, in fact, $z_n \in \mathcal{R}_{n+1}^o$ and $z_n' \in \mathcal{L}_{n+1}$.

Hence, by choosing the sign of each r_n for $n \geq 1$ so that it lies in the right half-plane (for all $n \geq 1$), we ensure that each $P_n = \wp_n(z_n)$, where $z_n \in \mathcal{R}_1^o$ does not depend on n. Hence the associated point sequence is coherent, as required.

For the last part, if $\Re r_n > 0$ only for $n > n_0 \geq 0$, then we simply apply the above argument to E_{n_0} and $(P_n)_{n \geq n_0}$, noting that P_{n_0} is a lift of P_0 to $E_{n_0}(\mathbb{C})$, and that every elliptic logarithm of P_{n_0} is also one of P_0. ☐

Lemma 27. *In the notation of Proposition 26, $\mathcal{R}_n^o \subset \mathcal{R}_{n+1}^o$ for all $n \geq 1$.*

Proof. It suffices to show that $\Re f_{n+1}(z)$ has constant sign for $z \in \mathcal{R}_n^o$, since this sign is positive for $z = w_1/2 \in \mathcal{R}_n^o$. If not, then there exists $z \in \mathcal{R}_n^o$ such that $\Re f_{n+1}(z) < 0$, so $f_{n+1}(z)^2$ is real and negative. We show this to be impossible.

We have

$$r_{n-1} = \frac{a_{n-2}r_n^2 - a_{n-1}}{-b_{n-2}r_n^2 + a_{n-1}} = h_n(r_{n-1}^2) = g_n(r_{n-1}),$$

say, where h_n is the linear fractional transformation

$$z \mapsto \frac{a_{n-2}z - a_{n-1}}{-b_{n-2}z + a_{n-1}},$$

and $g_n(z) = h_n(z^2)$. This implies that

$$f_n(z) = g_{n+1}(f_{n+1}(z)) = h_{n+1}(f_{n+1}(z)^2).$$

To complete the proof we show that the image of the negative real axis under h_n is contained in the left half-plane, for all $n \geq 1$. Let $t \in \mathbb{R}$ be negative, and set $s = 2t - 1 < -1$, and $\alpha = a_{n-2}/b_{n-2}$; then

$$h_n(t) = \frac{s\alpha - 1}{\alpha - s},$$

and we leave it to the reader to check that this has negative real part when $s < -1$ and $\Re\alpha > 0$. ☐

We remark that this lemma implies that we always have $\Re r_n > 0$ for $n \geq 2$. It is possible to have $\Re r_1 = 0$; this occurs if and only if x_0 lies on the open line segment between e_2 and e_3.

8.5 The elliptic logarithm algorithm

We summarise this section with the following algorithm.

Algorithm 28 (Complex Elliptic Logarithm)**.** Given an elliptic curve E defined over $\mathbb{C}$ by the Weierstrass equation $Y^2 = 4(X - e_1)(X - e_2)(X - e_3)$, and a non-2-torsion point $P \in E(\mathbb{C})$, compute an elliptic logarithm of P.

Input: E, with roots e_1, e_2, e_3, and $P = (x_0, y_0) \in E(\mathbb{C})$, with $y_0 \neq 0$.

1. Set $a_0 = \sqrt{e_1 - e_3}$ and $b_0 = \sqrt{e_1 - e_2}$, choosing the numbering of the roots (if necessary) and the signs so that $|a_0 - b_0| < |a_0 + b_0|$.
2. Set $r = \sqrt{(x_0 - e_3)/(x_0 - e_2)}$, with $\Re r \geq 0$.
3. Set $t = -y_0/(2r(x_0 - e_2))$ (so $t^2 = x_0 - e_1$).
4. Repeat the following, for $n = 1, 2, \ldots$:
   (a) set
   $$a_n = \frac{a_{n-1} + b_{n-1}}{2}, \quad b_n = \sqrt{a_{n-1}b_{n-1}},$$
   choosing the sign of b_n so that $|a_n - b_n| < |a_n + b_n|$;
   (b) set $r \leftarrow \sqrt{a_n(r+1)/(b_{n-1}r + a_{n-1})}$, with $\Re r > 0$.
   (c) set $t \leftarrow rt$.

   until $|a_n/b_n - 1|$ and $|r - 1|$ are sufficiently small. Set $M = \lim a_n$.

Output:
$$z_P = \frac{1}{M} \arctan\left(\frac{M}{t}\right).$$

Note that the output value of z_P may not be in the fundamental parallelogram of the period lattice Λ. However, assuming that the usual range for the arctan function is used, where $-\pi/2 < \Re \arctan(x) \leq \pi/2$, we will have $z_P = xw_1 + iyw_1$ with $x, y \in \mathbb{R}$ and $-1/2 < x \leq 1/2$.

For points P of order 2, choose the labelling of the roots so that $P = (e_1, 0)$ and then take $z_P = w_1/2 = \pi/(2M)$ where $M = M(\sqrt{e_1 - e_3}, \sqrt{e_1 - e_2})$.

8.6 The real case

For elliptic curves defined over $\mathbb{R}$ there is some advantage in adapting the algorithm to use real arithmetic where possible, even though the algorithm as given above works perfectly well in this situation. We divide into cases as in sections 6.2 and 6.3 above.

8.6.1 Curves with positive discriminant

Order the roots, which are all real, as in section 6.2, so that $e_1 > e_2 > e_3$; the real and imaginary periods w_1, w_2 are then given by (12).

Let $P = (x_0, y_0) \in E(\mathbb{R})$ with $2P \neq 0$ (so $y_0 \neq 0$). If P is in the connected component of the identity of $E(\mathbb{R})$ then $x_0 > e_1$, and it is immediate from the formulae given above that as well as all a_n, b_n being real and positive, so too are all r_n, and the t_n are real and with constant sign (opposite to that of y_0). Hence z_P, the output of the algorithm, is real and in the interval $|z_P| < w_1/2$.

Now suppose that $e_2 > x_0 > e_3$, so that P is in the other real component. Now $z_P = x_P + w_2/2$ where x_P is real, and it suffices to compute x_P. To do this we may replace P by $P' = P + (e_3, 0)$ which is in the identity component and has elliptic logarithm equal to x_P. A short calculation shows that we may compute x_P using the usual iteration, with the positive real initial values
$$r' = a_0/\sqrt{e_1 - x_0}; \qquad t' = r'y_0/2(x_0 - e_3).$$

8.6.2 Curves with negative discriminant

As in 6.3, we order the roots so that e_1 is real and $\Im e_2 > 0$. Set $a_0 = \sqrt{e_1 - e_3} = x + yi$ where $x, y > 0$. The real period is $w_1 = \pi/M(a_0, b_0) = \pi/M(x, R)$ where $R = |a_0|$. Now let $\sqrt{x_0 - e_3} = u + iv$ with $u, v > 0$, and then set the initial values of r and t to $r_1 = (u + iv)/(u - iv)$ and $t_1 = -y_0/2(u^2 + v^2)$.

Applying the first step in the iteration, we find that $a_1 = x$ and $b_1 = R$, and also that $r_2 = \sqrt{ux/(ux + vy)}$, where the quantity inside the square root is real and positive, so we may take $r_2 > 0$ also, and $t_2 = r_2 t_1$ which is also real and with the opposite sign to y_0. Now the rest of the iteration may be carried out using real values for all quantities, and again the output value z_P is real and satisfies $|z_P| < w_1/2$.

9 Examples

In the following examples, we will illustrate our method for computing the period lattices of elliptic curves over $\mathbb{C}$, and the elliptic logarithms of complex points. These examples were computed using the MAGMA implementation by the second author. All complex numbers in our examples are computed correctly up to 100 decimal places, but only the first 20 decimal places will be shown. Note that we implemented our own function for computing optimal AGM values, since the standard function in MAGMA does not always return an optimal one.

Example 1. Let E be the elliptic curve over $\mathbb{C}$ given by the Weierstrass equation

$$E: \quad Y^2 = 4(X - e_1)(X - e_2)(X - e_3)$$

with

$$e_1 = 3 - 2i, \quad e_2 = 1 + i, \quad e_3 = -4 + i.$$

Observe that $\sum_{j=1}^{3} e_j = 0$. We will compute the period lattice of E using the method described in Theorem 21. To do this, first we let $E_0 = E$ and calculate

$$a_0 = \sqrt{e_1 - e_3}, \quad b_0 = \sqrt{e_1 - e_2}, \quad c_0 = \sqrt{a_0^2 - b_0^2},$$

where the signs of a_0, b_0, c_0 are chosen so that (11) holds, i.e.

$$|a_0 - b_0| \le |a_0 + b_0|, \quad |a_0 - c_0| \le |a_0 + c_0|, \quad |c_0 - ib_0| \le |c_0 + ib_0|.$$

In this example, one can verify that such a_0, b_0, c_0 are

$$\begin{aligned} a_0 &= 2.70331029534753078867\ldots - i0.55487525889334275023\ldots \\ b_0 &= 1.67414922803554004044\ldots - i0.89597747612983812471\ldots \\ c_0 &= 2.23606797749978969640\ldots. \end{aligned}$$

In fact, all conditions in (11) are strictly inequalities in this case, so the period lattice of E is non-rectangular. By Theorem 21, we have

$$\begin{aligned} w_1 &= 1.29215151748713051904\ldots + i0.44759218107818896608\ldots \\ w_2 &= 1.42661373451784507587\ldots - i0.80963848056301882107\ldots \\ w_3 &= -0.13446221703071455682\ldots + i1.25723066164120778715\ldots \end{aligned}$$

and any two of w_j form a $\mathbb{Z}$-basis for Λ (where Λ is the period lattice of E). In our computation, we also have $|w_1 - w_2 - w_3| \approx 10^{-100}$. As expected, these w_j are minimal coset representatives of 2Λ in Λ.

Next, we wish to compute an elliptic logarithm of the point

$$P = (2 - i, 8 + 4i) \in E(\mathbb{C})$$

(which has infinite order). Using a_0, b_0 as above, Algorithm 28 gives

$$z_P = -0.72212997914002299126\ldots + i0.01717122412650902249\ldots.$$

Note that z_P is only well-defined modulo Λ. Depending on the basis for Λ, the value z_P obtained using Algorithm 28 may not lie in the fundamental parallelogram spanned by that basis. In our case, one can check that

$$\begin{aligned} z_P &= (-0.33249952362000772434\ldots)w_1 - (0.20502411273191295799\ldots)w_2 \\ &\equiv (0.66750047637999227565\ldots)w_1 + (0.79497588726808704200\ldots)w_2, \end{aligned}$$

and so z_P is not in the fundamental parallelogram spanned by $\{w_1, w_2\}$. Finally, one may verify that, to the given precision, we have, as expected,

$$\wp_\Lambda(z_P) = x(P), \quad \wp'_\Lambda(z_P) = y(P),$$

and

$$\wp_\Lambda(w_1/2) = e_1, \quad \wp_\Lambda(w_2/2) = e_2, \quad \wp_\Lambda(w_3/2) = e_3,$$

and $\wp'_\Lambda(w_j/2) \approx 0$ for all $j = 1, 2, 3$.

Example 2 (Rectangular Lattice)**.** Let E be the elliptic curve over $\mathbb{C}$ given the Weierstrass equation

$$E: \quad Y^2 = 4(X - e_1)(X - e_2)(X - e_3)$$

with

$$e_1 = 1 + 3i, \quad e_2 = -4 - 12i, \quad e_3 = 3 + 9i.$$

Observe that $\sum_{j=1}^{3} e_j = 0$ and all e_j are collinear. By letting $E_0 = E$ and computing a_0, b_0, c_0 as before, we have

$$\begin{aligned} a_0 &= 1.47046851723128684330\ldots - i2.04016608641756892919\ldots \\ b_0 &= -3.22578581905571472955\ldots - i2.32501487101070997214\ldots \\ c_0 &= 2.75099469475848456460\ldots - i3.81680125374499001591\ldots. \end{aligned}$$

This time, however, we have $|a_0 - b_0| = |a_0 + b_0|$, while the other two conditions in (11) are strictly inequalities. Hence we have two minimal elements (up to sign) in one coset of 2Λ in Λ (where Λ is the period lattice of E), and so Λ is rectangular.

To derive an orthogonal basis for Λ, first we let $w, w' = \pi/M(a_0, \pm b_0)$. In this example, we have

$$\begin{aligned} w &= -0.29920293143872535713\ldots + i1.10940038117892953702\ldots \\ w' &= 1.14708588706988127437\ldots + i0.06697438037476960963\ldots. \end{aligned}$$

One can check $|w| = |w'|$. Let $w_1 = (w + w')/2$ and $w_2 = (w - w')/2$. Then w_1, w_2 form an orthogonal basis for Λ, as proved in Lemma 5. Here, we have

$$\begin{aligned} w_1 &= 0.42394147781557795862\ldots + i0.58818738077684957333\ldots \\ w_2 &= -0.72314440925430331575\ldots + i0.52121300040207996369\ldots. \end{aligned}$$

Note that $\Re(w_2/w_1) = 0$, so both $\{w_1, w_2\}$ is indeed an orthogonal basis for Λ.

Let z_P be an elliptic logarithm of the point $P = (3 + 2i, 28 - 14i) \in E(\mathbb{C})$ (note that P has infinite order). Algorithm 28 shows that

$$\begin{aligned} z_P &= -0.42599662534207481578\ldots - i0.02491254923738153924\ldots \\ &\equiv (0.62858224538977667533\ldots)w_1 + (0.37134662195976180031\ldots)w_2. \end{aligned}$$

Finally, we verify that

$$|\wp_\Lambda(z_P) - x(P)| \approx 10^{-98}, \quad |\wp'_\Lambda(z_P) - y(P)| \approx 10^{-97}.$$

Moreover, we have

$$\begin{aligned} |\wp_\Lambda(w_1/2) - e_2| &\approx 10^{-99} \\ |\wp_\Lambda(w_2/2) - e_3| &\approx 0 \\ |\wp_\Lambda(w/2) - e_1| &\approx 10^{-99}, \end{aligned}$$

and

$$|\wp'_\Lambda(w_1/2)| \approx 10^{-99}, \quad |\wp'_\Lambda(w_2/2)| \approx 10^{-99}, \quad |\wp'_\Lambda(w/2)| \approx 10^{-100}.$$

Example 3. Let $K = \mathbb{Q}(\theta)$ where θ is a root of the polynomial $x^3 - 2$. Let E be the elliptic curve defined over K given by the Weierstrass equation

$$E: \quad Y^2 = 4(X - \theta)(X - 1)(X + 1 + \theta).$$

Note that K has one real embedding and one pair of complex embeddings. Let E_1, E_2 be the real and complex embedding of E respectively, i.e.

$$\begin{aligned} E_1: &\quad Y^2 = 4(X - \sqrt[3]{2})(X - 1)(X + 1 + \sqrt[3]{2}) \\ E_2: &\quad Y^2 = 4(X - \omega\sqrt[3]{2})(X - 1)(X + 1 + \omega\sqrt[3]{2}) \end{aligned}$$

where $\omega = \exp(2\pi i/3)$ is a cube root of unity. Since E_1 has three real roots, then the period lattice of E_1 is rectangular. In fact, by letting $e_1^{(0)} = \sqrt[3]{2}, e_2^{(0)} = 1, e_3^{(0)} = -1 - \sqrt[3]{2}$, we can compute a_0, b_0, c_0 satisfying (11) as

$$\begin{aligned} a_0 &= 1.87612422291002530767\ldots \\ b_0 &= 0.50982452853395859808\ldots \\ c_0 &= 1.80552514518487755254\ldots. \end{aligned}$$

One can then verify that $|c_0 - ib_0| = |c_0 + ib_0|$. As before, we compute

$$w = \frac{\pi}{M(c_0, ib_0)} = 2.90130425944817643666\ldots - i1.70677932803214980295\ldots$$

$$w' = \frac{\pi}{M(c_0, -ib_0)} = \bar{w},$$

and let $w_1, w_2 = (w \pm w')/2$. Then w_1, w_2 form an orthogonal basis for the period lattice of E_1. In this example, we have $w_1 = \Re(w)$ and $w_2 = i\Im(w)$.

Nevertheless, the period lattice of E_2 is non-rectangular, since all roots of E_2 are not collinear. In fact, by letting $e_1^{(0)} = -1 - \omega\sqrt[3]{2}, e_2^{(0)} = 1, e_3^{(0)} = \omega\sqrt[3]{2}$ (here we must ensure that a_0, b_0, c_0 satisfy (11)), we have

$$\begin{aligned} a_0 &= 1.10851094368231305521\ldots - i0.98431471713501219051\ldots \\ b_0 &= 0.43669517024285334726\ldots - i1.24929666083200513980\ldots \\ c_0 &= 1.34004098848655674756\ldots - i0.40712323180652750769\ldots. \end{aligned}$$

One can check that all conditions in (11) are strictly inequalities, hence this also confirms that the period lattice of E_2 is non-rectangular. By Theorem 21, we finally obtain

$$\begin{aligned} w_1 &= 1.28194824894788708942\ldots + i1.88277404359595361782\ldots \\ w_2 &= 2.36557653380849535471\ldots - i0.03808700290170419307\ldots \\ w_3 &= -1.08362828486060826529\ldots + i1.92086104649765781090\ldots \end{aligned}$$

with $|w_1 - w_2 - w_3| \approx 10^{-100}$.

Example 4. Let E be the elliptic curve over $\mathbb{C}$ given by the Weierstrass equation

$$E: \quad Y^2 = 4(X - e_1)(X - e_2)(X - e_3)$$

with

$$e_1 = -1 - 3i, \quad e_2 = 3 + i, \quad e_3 = -2 + 2i.$$

Observe that $\sum_{j=1}^{3} e_j = 0$ and $|e_1 - e_3| = |e_2 - e_3|$. Thus e_1, e_2, e_3 are on an isosceles triangle. By letting $E_0 = E$ and computing a_0, b_0, c_0 as before, we have

$$\begin{aligned} a_0 &= 1.74628455779589152702\ldots - i1.43161089573822132705\ldots \\ b_0 &= 0.91017972112445468260\ldots - i2.19736822693561993207\ldots \\ c_0 &= 2.24711142509587014360\ldots - i0.22250788030178260411\ldots. \end{aligned}$$

Hence by Theorem 21, we obtain

$$\begin{aligned} w_1 &= 0.81646689790312614904\ldots + i1.10773333340066743861\ldots \\ w_2 &= 1.36061503191563570645\ldots - i0.20595647167234558716\ldots \\ w_3 &= -0.54414813401250955741\ldots + i1.31368980507301302578\ldots \end{aligned}$$

with $|w_1 - w_2 - w_3| \approx 10^{-100}$. In addition, one can check that $\Re(w_1/w_3) = 1/2$ as claimed in Section 6.3. Let Λ be the period lattice of E. We finally verify that $|\wp_\Lambda(w_j/2) - e_j| \approx 10^{-100}$ for all $j = 1, 2, 3$, and

$$|\wp'_\Lambda(w_1/2)| \approx 10^{-99}, \quad |\wp'_\Lambda(w_2/2)| \approx 10^{-100}, \quad |\wp'_\Lambda(w_3/2)| \approx 10^{-99}.$$

References

[1] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. J. Symbolic Comput., **24(3-4)** (1997), 235–265.

[2] J.-B. Bost and J.-F. Mestre, *Moyenne arithmético-géométrique et périodes des courbes de genre* 1 *et* 2, Gaz. Math. **38** (1988), 36–64.

[3] H. Cohen, *A course in computational algebraic number theory*, Grad. Texts in Math., **138**, Springer-Verlag, 1993.

[4] D. A. Cox, *The arithmetic-geometric mean of Gauss*, Enseign. Math. (2) **30** (1984), 275–330.

[5] J. E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, 1997.

[6] R. Dupont, *Fast evaluation of modular functions using Newton iterations and the AGM*, preprint available at `http://www.lix.polytechnique.fr/Labo/Regis.Dupont/`.

[7] H. Geppert, *Zur Theorie des arithmetisch-geometrischen Mittels*, Math. Ann. **99** (1928), 162–180.

[8] W. A. Stein et al., *Sage Mathematics Software (Version 4.5.3)*, The Sage Development Team, 2010, `http://www.sagemath.org`.

[9] T. Thongjunthug, *Height bounds for elliptic curves over number fields, periods and complex elliptic logarithms*, University of Warwick PhD thesis, to be submitted.