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

John Cremona

University of Warwick

Sage Days 23, Leiden
8 July 2010

Plan

1. Introduction and statement of the problem
2. AGM sequences, lattice chains and isogeny chains
3. Periods of elliptic curves over $\mathbb{C}$
4. Complex elliptic logarithms
5. Local heights at complex places (work in progress)

Joint work with Thotsaphon Thongjunthug (Warwick)

Plan

1. Introduction and statement of the problem
2. AGM sequences, lattice chains and isogeny chains
3. Periods of elliptic curves over $\mathbb{C}$
4. Complex elliptic logarithms
5. Local heights at complex places (work in progress)

Joint work with Nook (Warwick)

We will study three related classes of objects:

- Complex AGM sequences (first studied by Gauss!)
- Chains of lattices in $\mathbb{C}$
- Chains of 2-isogenies between elliptic curves over $\mathbb{C}$

We will study three related classes of objects:

- Complex AGM sequences (first studied by Gauss!)
- Chains of lattices in $\mathbb{C}$
- Chains of 2-isogenies between elliptic curves over $\mathbb{C}$

in order to give efficient computational solutions to these questions:

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

The real AGM

Let a, b be *positive real* numbers. Set $a_0 = 1$, $b_0 = b$, and for all $n \geq 0$,

$$a_{n+1} = +\frac{1}{2}(a_n + b_n), \quad b_{n+1} = +\sqrt{a_n b_n}.$$

Then $\lim a_n$ and $\lim b_n$ both exist and are equal. Their common value is the *Arithmetic-Geometric Mean* $M(a, b)$.

The real AGM

Let a, b be *positive real* numbers. Set $a_0 = 1$, $b_0 = b$, and for all $n \geq 0$,

$$a_{n+1} = +\frac{1}{2}(a_n + b_n), \quad b_{n+1} = +\sqrt{a_n b_n}.$$

Then $\lim a_n$ and $\lim b_n$ both exist and are equal. Their common value is the *Arithmetic-Geometric Mean* $M(a, b)$.

The AGM is well known and has been used for centuries in evaluating (real) elliptic integrals. For example:

$$\int_0^{\pi/2} \frac{dx}{\sqrt{a^2 \cos^2 x + b^2 \sin^2 x}} = \frac{\pi}{2M(a, b)}.$$

Complex AGM sequences

We now consider pairs $a, b \in \mathbb{C}$ such that $ab(a^2 - b^2) \neq 0$.

A pair is *good* if $|a - b| \leq |a + b|$, or equivalently $\Re(a/b) \geq 0$.

Complex AGM sequences

We now consider pairs $a, b \in \mathbb{C}$ such that $ab(a^2 - b^2) \neq 0$.

A pair is *good* if $|a-b| \leq |a+b|$, or equivalently $\Re(a/b) \geq 0$.

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

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

for all $n \geq 0$.

Complex AGM sequences

We now consider pairs $a, b \in \mathbb{C}$ such that $ab(a^2 - b^2) \neq 0$.

A pair is *good* if $|a - b| \leq |a + b|$, or equivalently $\Re(a/b) \geq 0$.

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

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

for all $n \geq 0$.

There are uncountably many AGM sequences starting with (a_0, b_0).

$a_{n+1} = (a_n + b_n)/2$ and $b_{n+1} = \pm\sqrt{a_n b_n}$, with either choice of sign at each step.

Good sequences and optimality

An AGM sequence is

- *good* if (a_n, b_n) is good for all but finitely many n, else *bad*;
- *optimal* if (a_n, b_n) is good for all $n > 0$;
- *strongly optimal* if (a_n, b_n) is good for all $n \geq 0$;

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.

These have the property that the ratios a_n/b_n in one of the sequences are the complex conjugates of those in the other.

Limits of AGM sequences

All AGM sequences have limits. More precisely:

For every AGM sequence $((a_n, b_n))_{n=0}^{\infty}$ starting at (a_0, b_0):

1. $\lim_{n\to\infty} a_n$ and $\lim_{n\to\infty} b_n$ exist and are equal;
2. The common limit M is non-zero iff the sequence is good;
3. $|M|$ attains its maximum iff the sequence is optimal.

Limits of AGM sequences

All AGM sequences have limits. More precisely:

For every AGM sequence $((a_n, b_n))_{n=0}^{\infty}$ starting at (a_0, b_0):

1. $\lim_{n\to\infty} a_n$ and $\lim_{n\to\infty} b_n$ exist and are equal;
2. The common limit M is non-zero iff the sequence is good;
3. $|M|$ attains its maximum iff the sequence is optimal.

The first two parts of this are elementary. The third (harder) implies

$$|M(a,b)| \geq |M(a,-b)| \iff |a-b| \leq |a+b|.$$

Lattices and lattice chains

A *lattice* is a discrete free rank 2 $\mathbb{Z}$-module in $\mathbb{C}$.

A *lattice chain* is an infinite nested sequence of lattices

$$\Lambda_0 \supset \Lambda_1 \supset \Lambda_2 \supset \cdots \supset \Lambda_n \supset \dots$$

such that $[\Lambda_n : \Lambda_{n+1}] = 2$ and $\Lambda_{n+1} \neq 2\Lambda_{n-1}$ for all $n \geq 1$ (so Λ_0/Λ_n is cyclic of order 2^n).

Lattices and lattice chains

A *lattice* is a discrete free rank 2 $\mathbb{Z}$-module in $\mathbb{C}$.

A *lattice chain* is an infinite nested sequence of lattices

$$\Lambda_0 \supset \Lambda_1 \supset \Lambda_2 \supset \cdots \supset \Lambda_n \supset \dots$$

such that $[\Lambda_n : \Lambda_{n+1}] = 2$ and $\Lambda_{n+1} \neq 2\Lambda_{n-1}$ for all $n \geq 1$ (so Λ_0/Λ_n is cyclic of order 2^n).

For each $n \geq 1$ we have $\Lambda_{n+1} = \langle w \rangle + 2\Lambda_n$ for some $w \in \Lambda_n \setminus 2\Lambda_{n-1}$.

Given Λ_0, there are *three* possibilities for Λ_1, and then *two* choices for Λ_n for $n \geq 2$.

The number of such chains starting with Λ_0 is uncountable.

Good lattice chains and limiting periods

Let

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

Then one of two possibilities occurs (since Λ_∞ has infinite index):

- if $\Lambda_\infty = \{0\}$, the chain is *bad*;
- if Λ_∞ is free of rank 1, the chain is *good*.

Good lattice chains and limiting periods

Let

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

Then one of two possibilities occurs (since Λ_∞ has infinite index):

- if $\Lambda_\infty = \{0\}$, the chain is *bad*;
- if Λ_∞ is free of rank 1, the chain is *good*.

In a good chain, $\Lambda_\infty = \langle w_\infty \rangle$ for some *primitive* period w_∞, called a *limiting period* of the chain.

Good and bad choices in lattice chains

$\Lambda_{n+1} \subset \Lambda_n$ 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).

Good and bad choices in lattice chains

$\Lambda_{n+1} \subset \Lambda_n$ 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).

For a good chain $(\Lambda_n)_{n=0}^{\infty}$, the limiting period w_∞ is minimal in Λ_n for all but finitely many $n \geq 0$.

A chain is good if and only if $\Lambda_{n+1} \subset \Lambda_n$ is the right choice for all but finitely many $n \geq 1$.

Optimal chains

A lattice chain is *optimal* if $\Lambda_{n+1} \subset \Lambda_n$ is the right choice for *all* $n \geq 1$.

There is usually *one* optimal chain for each of the three choices of Λ_1.

Optimal chains

A lattice chain is *optimal* if $\Lambda_{n+1} \subset \Lambda_n$ is the right choice for *all* $n \geq 1$.

There is usually *one* optimal chain for each of the three choices of Λ_1.

More precisely, a good chain is optimal if and only if w_∞ is a *minimal coset representative* of $2\Lambda_0$ in Λ_0; and the only situation in which minimal coset representatives are not unique (up to sign) is for *rectangular lattices* where the “diagonal” coset has a pair of minimal representatives (up to sign).

When Λ_0 is rectangular with orthogonal basis w_1, w_2 there are *four* optimal chains, including *two* with $\Lambda_1 = \langle w_1 + w_2 \rangle + 2\Lambda_0$.

Coset representatives and $\mathbb{Z}$-bases

A good chain of lattices with limiting period w_∞ is optimal if and only if w_∞ is a minimal coset representative of $2\Lambda_0$ in Λ_0.

Coset representatives and $\mathbb{Z}$-bases

A good chain of lattices with limiting period w_∞ is optimal if and only if w_∞ is a minimal coset representative of $2\Lambda_0$ in Λ_0.

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.

Coset representatives and $\mathbb{Z}$-bases

A good chain of lattices with limiting period w_∞ is optimal if and only if w_∞ is a minimal coset representative of $2\Lambda_0$ in Λ_0.

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.

We will need these results to show that our AGM-based algorithm not only finds individual primitive periods, but actually gives a $\mathbb{Z}$-basis for the period lattice. This uses one more easy fact:

For $j = 1, 2, 3$, let w_j be minimal coset representatives for 2Λ in Λ. Then any two of the w_j form a $\mathbb{Z}$-basis for Λ.

Level 4 structure

We link AGM sequences with lattice chains via level 4 structure on elliptic curves and 2-isogenies.

There are bijections between the following sets:

1. “short” lattice chains $\Lambda_0 \supset \Lambda_1 \supset \Lambda_2$ 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 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.

Level 4 structure

We link AGM sequences with lattice chains via level 4 structure on elliptic curves and 2-isogenies.

There are bijections between the following sets:

1. "short" lattice chains $\Lambda_0 \supset \Lambda_1 \supset \Lambda_2$ 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 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.

$(1) \leftrightarrow (2)$ is clear. For $(2) \leftrightarrow (3)$ we use the elliptic curve

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

on which $P_{\{a,b\}} = (ab, 2ab(a + b))$ has order 4 and $2P = T = (0, 0)$.

Modular functions

Up to homothety our level 4 structures are parametrized by points τ in the affine modular curve $Y_0(4) = \Gamma_0(4)\backslash\mathcal{H}$ where $\mathcal{H}$ is the upper half-plane.

The ratio a/b is a modular function (of τ).

Modular functions

Up to homothety our level 4 structures are parametrized by points τ in the affine modular curve $Y_0(4) = \Gamma_0(4)\backslash\mathcal{H}$ where $\mathcal{H}$ is the upper half-plane.

The ratio a/b is a modular function (of τ). In fact,

- $\tau \mapsto \kappa(\tau) = a/b$ is a hauptmodul for $\Gamma_0(4) \cap \Gamma(2)$;
- $\tau \mapsto \lambda(\tau) = a^2/b^2$ is a hauptmodul for $\Gamma(2)$;
- $\tau \mapsto f(\tau) = a/b + b/a$ is a hauptmodul for $\Gamma_0(4)$;
- $$f(\tau) = 2(1 + \lambda(2\tau))/(1 - \lambda(2\tau))$$

  where $\lambda(\tau)$ is the classical Legendre elliptic function on $\Gamma(2)$.

Application of modular functions

By studying the values taken by the modular function f on the upper half-plane, one can prove:

Theorem

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. The following are equivalent:

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

The link: isogeny chains

Let Λ_0 be the period lattice of an elliptic curve $E_0/\mathbb{C}$ with Weierstrass equation

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

Let

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

Fixing the order and signs of a_0, b_0 corresponds to fixing a point P of order 4 on E_0 with $2P = T = (e_1^{(0)}, 0)$, and to fixing a short lattice chain $\Lambda_0 \supset \Lambda_1 \supset \Lambda_2$.

AGM sequences $((a_n, b_n))_{n=0}^{\infty}$ starting from (a_0, b_0) now correspond to lattice chains (Λ_n) with the same three starting terms.

The link: isogeny chains

For each $n \geq 0$ let

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

and E_n the curve with equation $Y_n^2 = 4(X_n - e_1^{(n)})(X_n - e_2^{(n)})(X_n - e_3^{(n)})$.

The link: isogeny chains

For each $n \geq 0$ let

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

and E_n the curve with equation $Y_n^2 = 4(X_n - e_1^{(n)})(X_n - e_2^{(n)})(X_n - e_3^{(n)})$.

Λ_n is the period lattice of E_n and there are 2-isogenies $\varphi_n : E_n \to E_{n-1}$ induced by $\mathbb{C}/\Lambda_n \to \mathbb{C}/\Lambda_{n-1}$, which fit together to form an isogeny chain:

$$\cdots \longrightarrow E_n \xrightarrow{\varphi_n} E_{n-1} \longrightarrow \cdots \longrightarrow E_1 \longrightarrow E_0$$

where $\varphi_n((e_1^{(n)}, 0)) = (e_1^{(n-1)}, 0)$ for all $n \geq 1$.

The limit

Assume that the AGM sequence (a_n, b_n) is good, with nonzero limit M. Then

$$\lim_{n\to\infty} e_1^{(n)} = \frac{2}{3}M^2; \qquad \lim_{n\to\infty} e_2^{(n)} = \lim_{n\to\infty} e_3^{(n)} = \frac{-1}{3}M^2.$$

The limit

Assume that the AGM sequence (a_n, b_n) is good, with nonzero limit M. Then

$$\lim_{n\to\infty} e_1^{(n)} = \frac{2}{3}M^2; \qquad \lim_{n\to\infty} e_2^{(n)} = \lim_{n\to\infty} e_3^{(n)} = \frac{-1}{3}M^2.$$

Equivalently, the lattice chain (Λ_n) is good, with limiting period w_∞:

$$\begin{tikzcd}
\mathbb{C} \arrow[d] & \cdots \arrow[l] & \mathbb{C} \arrow[l] \arrow[d] & \mathbb{C} \arrow[l, "\mathrm{id}"'] \arrow[d] & \cdots \arrow[l] & \mathbb{C} \arrow[l] \arrow[d] \\
\mathbb{C}/\Lambda_0 \arrow[d] & \cdots \arrow[l] & \mathbb{C}/\Lambda_n \arrow[l] \arrow[d, "\wp_n"] & \mathbb{C}/\Lambda_{n+1} \arrow[l] \arrow[d, "\wp_{n+1}"] & \cdots \arrow[l] & \mathbb{C}/\langle w_\infty \rangle \arrow[l] \arrow[d] \\
E_0 & \cdots \arrow[l] & E_n \arrow[l] & E_{n+1} \arrow[l, "\varphi_n"] & \cdots \arrow[l] & E_\infty \arrow[l]
\end{tikzcd}$$

where E_∞ is the singular curve $Y^2 = 4(X - 2M^2/3)(X + M^2/3)^2$.

Summary so far

We have established bijections between three sets:

1. all AGM sequences starting at (a_0, b_0);
2. all isogeny chains starting with the short chain $E_2 \to E_1 \to E_0$;
3. all lattice chains starting with the short chain $\Lambda_0 \supset \Lambda_1 \supset \Lambda_2$.

Summary so far

We have established bijections between three sets:

1. all AGM sequences starting at (a_0, b_0);
2. all isogeny chains starting with the short chain $E_2 \to E_1 \to E_0$;
3. all lattice chains starting with the short chain $\Lambda_0 \supset \Lambda_1 \supset \Lambda_2$.

such that for all n,

1. $E_n \cong E_{\{a_n, b_n\}} \cong \mathbb{C}/\Lambda_n$;
2. $\Lambda_n \supset \Lambda_{n+1} \supset \Lambda_{n+2}$ is a short chain;
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).

Computing periods via AGM

We now show how every primitive period w_1 of E_0 may be expressed in terms of the limit of a suitable AGM sequence.

w_1 determines a good lattice chain with $\Lambda_n = \langle w_1 \rangle + 2^n \Lambda_0$ (and conversely, since $\cap_n \Lambda_n = \langle w_1 \rangle$).

The lattice chain in turn determines a good AGM sequence $((a_n, b_n))$ starting at a pair (a_0, b_0) such that $E_0 \cong E_{\{a_0, b_0\}}$.

Computing periods via AGM

We now show how every primitive period w_1 of E_0 may be expressed in terms of the limit of a suitable AGM sequence.

w_1 determines a good lattice chain with $\Lambda_n = \langle w_1 \rangle + 2^n \Lambda_0$ (and conversely, since $\cap_n \Lambda_n = \langle w_1 \rangle$).

The lattice chain in turn determines a good AGM sequence $((a_n, b_n))$ starting at a pair (a_0, b_0) such that $E_0 \cong E_{\{a_0, b_0\}}$.

Theorem

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

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

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

The period formula

Taking $z = w_1/2$ we find:

Corollary

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. Then $M = \pm\pi/w_1$, so that the period w_1 may be determined up to sign by

$$w_1 = \pm\pi/M.$$

The period formula

Taking $z = w_1/2$ we find:

Corollary

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*. Then* $M = \pm\pi/w_1$*, so that the period* w_1 *may be determined up to sign by*

$$w_1 = \pm\pi/M.$$

Choosing different good AGM sequences we obtain all primitive periods in the coset $w_1 + 4\Lambda_0$*; the optimal sequence's limit gives the minimal such period.*
Choosing the sign of b_0 *so that* (a_0, b_0) *is good, the strongly optimal AGM sequence's limit gives the minimal period in the same coset* $w_1 + 2\Lambda_0$*.*

Another corollary

Corollary

$|\operatorname{AGM}(a_0, b_0)|$ attains its maximum among all limits of AGM-sequences starting at (a_0, b_0) if and only if the sequence is optimal.

Conclusion: computing periods I

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

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

where the signs are chosen so that (a_0, b_0) is good, i.e.,

$$|a_0 - b_0| \le |a_0 + b_0|,$$

and let

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

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.

Conclusion: computing periods II

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

$$|a-b| \le |a+b|, \quad |c-ib| \le |c+ib|, \quad |a-c| \le |a+c|.$$

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.

Special Case I: Real Curves with $\Delta > 0$

Here the e_j are all real and we may order them so that $e_1 > e_2 > e_3$.

We obtain a rectangular basis for the period lattice by setting

$$\begin{aligned} w_1 &= \pi / \operatorname{AGM}(\sqrt{e_1 - e_2}, \sqrt{e_1 - e_3}), \\ w_2 &= \pi i / \operatorname{AGM}(\sqrt{e_2 - e_3}, \sqrt{e_1 - e_3}) \end{aligned}$$

with all square roots positive; then w_1 and w_2/i are both real and positive.

Special Case II: Real Curves with $\Delta < 0$

Order the roots so that $e_1 \in \mathbb{R}$ and $e_2 = \overline{e_3}$.

Set $a_0 = \sqrt{e_1 - e_3} = x + yi$; we may assume that $x, y > 0$ by swapping e_2, e_3 or changing the sign of a_0 if necessary. Set $r = \sqrt{x^2 + y^2} > 0$ and $b_0 = \sqrt{e_1 - e_2} = x - yi$. Now

$$w_+ = \pi/\operatorname{AGM}(a_0, b_0) = \pi/\operatorname{AGM}(x + yi, x - yi) = \pi/\operatorname{AGM}(x, r)$$

is a real period, and

$$w_- = \pi/\operatorname{AGM}(-a_0, b_0) = \pi i/\operatorname{AGM}(y - xi, y + xi) = \pi i/\operatorname{AGM}(y, r).$$

is an imaginary period.

These periods span a sublattice of index 2 in the period lattice, for which a $\mathbb{Z}$-basis may be taken to be

$$w_1 = w_+ \qquad \text{and} \qquad w_2 = (w_+ + w_-)/2,$$

with $\Re(w_2/w_1) = 1/2$.

The problem

We wish to invert the map

$$\mathbb{C} \longrightarrow \mathbb{C}/\Lambda \xrightarrow{\wp_\Lambda} E(\mathbb{C}).$$

The *elliptic logarithm* of $P = (x, y) \in E(\mathbb{C})$ is any $z \in \mathbb{C}$ such that

$$\wp_\Lambda(z) := (\wp(z; \Lambda), \wp'(z; \Lambda)) = (x, y).$$

Recall the diagram:

$$\begin{tikzcd}
\mathbb{C} \arrow[d] & \cdots \arrow[l] & \mathbb{C} \arrow[l] \arrow[d] & \mathbb{C} \arrow[l, "\mathrm{id}"'] \arrow[d] & \cdots \arrow[l] & \mathbb{C} \arrow[l] \arrow[d] \\
\mathbb{C}/\Lambda_0 \arrow[d] & \cdots \arrow[l] & \mathbb{C}/\Lambda_n \arrow[l] \arrow[d, "\wp_n"] & \mathbb{C}/\Lambda_{n+1} \arrow[l] \arrow[d, "\wp_{n+1}"] & \cdots \arrow[l] & \mathbb{C}/\langle w_\infty \rangle \arrow[l] \arrow[d] \\
E_0 & \cdots \arrow[l] & E_n \arrow[l] & E_{n+1} \arrow[l, "\varphi_n"] & \cdots \arrow[l] & E_\infty \arrow[l]
\end{tikzcd}$$

Given $z \in \mathbb{C}$ define $P_n = \wp_n(z)$ for $n \geq 0$.

Then $\varphi_n(P_{n+1}) = P_n$ for $n \geq 0$.

If $\lim P_n = (x_\infty, y_\infty)$ then one can recover z from x_∞, y_∞ using formulae given earlier for $\lim \wp_n(z), \lim \wp'_n(z)$.

Coherent sequences

Conversely, to each $P = P_0 \in E_0(\mathbb{C})$ there are uncountably many such "coherent sequences" (P_n), of which only a countable number arise in this way, one for each choice of z with $\wp_0(z) = P_0$. (These z values form a whole coset of Λ_0 in $\mathbb{C}$.) We call the latter "good sequences".

Coherent sequences

Conversely, to each $P = P_0 \in E_0(\mathbb{C})$ there are uncountably many such "coherent sequences" (P_n), of which only a countable number arise in this way, one for each choice of z with $\wp_0(z) = P_0$. (These z values form a whole coset of Λ_0 in $\mathbb{C}$.) We call the latter "good sequences".

We will recursively compute the point sequence $(P_n) = ((x_n, y_n))$ from $P = (x, y)$. At each stage there will be two choice of preimage $P_{n+1} \in \varphi_n^{-1}(P_n)$. Of these, we can specify one as the "right choice" in such a way that the countable number of good sequences are exactly those in which all but a finite number of choices are right.

Choices

To any coherent sequence (P_n) we associate the nested sequence of cosets $C_n = z_n + \Lambda_n$, where z_n is any elog of P_n.

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

Each Λ_n-coset C_n splits into two Λ_{n+1}-cosets, one of which is C_{n+1}.

Choices

To any coherent sequence (P_n) we associate the nested sequence of cosets $C_n = z_n + \Lambda_n$, where z_n is any elog of P_n.

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

Each Λ_n-coset C_n splits into two Λ_{n+1}-cosets, one of which is C_{n+1}.

The point sequence is good if and only if $\cap C_n \neq \emptyset$. In this case the intersection is a coset of Λ_∞.

The *right choice* of C_{n+1} (or equivalently of P_{n+1}) is the one containing the *minimal* element of C_n.

Discreteness implies that $\cap C_n \neq \emptyset$ iff C_{n+1} is the right choice for all but finitely many n.

New coordinates

It turns out to yield simpler formulae if instead of coordinates (x_n, y_n) on E_n we use coordinates (t_n, u_n, v_n) where

$$\begin{aligned} t_n^2 + e_1^{(n)} = u_n^2 + e_2^{(n)} = v_n^2 + e_3^{(n)} &= x_n \\ 2t_n u_n v_n &= y_n. \end{aligned}$$

New coordinates

It turns out to yield simpler formulae if instead of coordinates (x_n, y_n) on E_n we use coordinates (t_n, u_n, v_n) where

$$\begin{aligned} t_n^2 + e_1^{(n)} = u_n^2 + e_2^{(n)} = v_n^2 + e_3^{(n)} &= x_n \\ 2t_n u_n v_n &= y_n. \end{aligned}$$

The formula for the 2-isogeny now gives

$$\begin{aligned} u_n &= \frac{1}{2}(u_{n-1} + v_{n-1}), \\ v_n &= \pm\sqrt{u_n^2 - a_n^2 + b_n^2}, \\ t_n &= \frac{u_n t_{n-1}}{v_n}. \end{aligned}$$

and the "right choice" is to take $|v_n - u_n| \leq |v_n + u_n|$.

The elliptic logarithm algorithm

Input: An elliptic curve E defined over $\mathbb{C}$, with roots e_1, e_2, e_3;
a point $P = (x, y) \in E(\mathbb{C})$ with $y \neq 0$.

1. Let $a_0 = \sqrt{e_1 - e_3}$ and $b_0 = \sqrt{e_1 - e_2}$.
   Choose the sign of b_0 so that $|a_0 - b_0| \leq |a_0 + b_0|$.
2. Let $u_0 = \sqrt{x - e_3}$ and $v_0 = \sqrt{x - e_2}$.
   Choose the sign of v_0 so that $|u_0 - v_0| \leq |u_0 + v_0|$.
3. Let $t_0 = -y/(2u_0v_0)$.

4. Set $n = 1$. Repeat the following:
   1. Let
      $$a_n = \frac{a_{n-1} + b_{n-1}}{2}, \quad b_n = \sqrt{a_{n-1}b_{n-1}}, \quad c_n = \sqrt{a_n^2 - b_n^2}.$$
      Choose the sign of b_n so that $|a_n - b_n| \leq |a_n + b_n|$.
   2. Let $u_n = (u_{n-1} + v_{n-1})/2$ and $v_n = \sqrt{u_n^2 - c_n^2}$.
      Choose the sign of v_n so that $|u_n - v_n| \leq |u_n + v_n|$.
   3. Let $t_n = u_n t_{n-1}/v_n$.
   4. $n \leftarrow n + 1$.

4. Set $n = 1$. Repeat the following:
   1. Let
   $$a_n = \frac{a_{n-1} + b_{n-1}}{2}, \quad b_n = \sqrt{a_{n-1}b_{n-1}}, \quad c_n = \sqrt{a_n^2 - b_n^2}.$$
   Choose the sign of b_n so that $|a_n - b_n| \leq |a_n + b_n|$.
   2. Let $u_n = (u_{n-1} + v_{n-1})/2$ and $v_n = \sqrt{u_n^2 - c_n^2}$.
   Choose the sign of v_n so that $|u_n - v_n| \leq |u_n + v_n|$.
   3. Let $t_n = u_n t_{n-1}/v_n$.
   4. $n \leftarrow n + 1$.
5. Let $M = \lim a_n$ and $T = \lim t_n$.

4. Set $n = 1$. Repeat the following:
   1. Let
   $$a_n = \frac{a_{n-1} + b_{n-1}}{2}, \quad b_n = \sqrt{a_{n-1}b_{n-1}}, \quad c_n = \sqrt{a_n^2 - b_n^2}.$$
   Choose the sign of b_n so that $|a_n - b_n| \le |a_n + b_n|$.
   2. Let $u_n = (u_{n-1} + v_{n-1})/2$ and $v_n = \sqrt{u_n^2 - c_n^2}$.
   Choose the sign of v_n so that $|u_n - v_n| \le |u_n + v_n|$.
   3. Let $t_n = u_n t_{n-1}/v_n$.
   4. $n \leftarrow n + 1$.
5. Let $M = \lim a_n$ and $T = \lim t_n$.

Output:

$$z_P = \frac{1}{M} \arctan\left(\frac{M}{T}\right).$$

Implementations

We have implemented the algorithm in both SAGE and MAGMA.

The Sage version (by JEC) was merged in version 4.4 of Sage after ticket #6390 was positively reviewed by Chris Wüthrich. We also needed to re-implement the complex AGM since previously SAGE used PARI/GP's `agm` function, which does not give "optimal" values. That was done jointly by JEC and Robert Bradshaw (in Cython for efficiency).

Implementations

We have implemented the algorithm in both SAGE and MAGMA.

The Sage version (by JEC) was merged in version 4.4 of Sage after ticket #6390 was positively reviewed by Chris Wüthrich. We also needed to re-implement the complex AGM since previously SAGE used PARI/GP's `agm` function, which does not give "optimal" values. That was done jointly by JEC and Robert Bradshaw (in Cython for efficiency).

The Magma version was implemented by TT, who also provided the examples.

We will only give one example here. For more examples, see `http://www.sagemath.org/doc/reference/sage/schemes/elliptic_curves/period_lattice.html`!

Example

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

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

Example

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

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

Now

$$a_0 = 2.70331029534753078867\ldots - i0.55487525889334275023\ldots$$
$$b_0 = 1.67414922803554004044\ldots - i0.89597747612983812471\ldots$$
$$c_0 = 2.23606797749978969640\ldots$$

satisfy

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

and

$$|a_1 - b_1| < |a_1 + b_1|, \quad |c_1 - ib_0| < |c_0 + ib_0|, \quad |a_0 - c_0| < |a_0 + c_0|.$$

Example (continued)

The minimal periods are

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

any two of w_j form a $\mathbb{Z}$-basis for Λ, the period lattice of E.

Example (continued)

The minimal periods are

$$w_1 = 1.29215151748713051904\ldots + i0.44759218107818896608\ldots,$$
$$w_2 = 1.42661373451784507587\ldots - i0.80963848056301882107\ldots,$$
$$w_3 = -0.13446221703071455682\ldots + i1.25723066164120778715\ldots;$$

any two of w_j form a $\mathbb{Z}$-basis for Λ, the period lattice of E.

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

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

(which has infinite order). We find

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

Canonical heights

If E is an elliptic curve defined over a number field K, then the *canonical* or *Néron-Tate height* of of K of *local heights*.

At finite (non-archimedean) places this is easy to compute.

At real and complex places there are several methods available.

Mestre showed how to use real AGM sequences (and the same chain of 2-isogenies as for computing periods) to compute the local height of a point at a real place.

Complex local heights

Using complex AGM sequences, we are extending Mestre's method to an algorithm for computing local heights at complex places.

As with all AGM-based methods, the convergence is very fast, allowing for very high precision to be attained easily.

One problem: for the elliptic log algorithm there are many "correct" answers since the elliptic log is only well-defined modulo the period lattice. In some ways it does not matter which representative value the algorithm produces.

However, the local height is a uniquely determined number: so we have to be very careful to determine exactly what the effect of taking different choices in the AGM sequences is.

This work is still in progress!

Hup Holland hup

Hup Holland hup!
Laat de leeuw niet in z'n hempie staan
Hup Holland hup!
Trek het beessie geen pantoffels aan
Hup Holland hup!
Laat je uit 't veld niet slaan
Want de leeuw op voetbalschoenen
Durft de hele wereld aan