

A Complete Arithmetic-Geometric Mean for E/\mathbb{C}

Eleanor Farrington

Abstract. The relation between elliptic curves and the arithmetic-geometric mean was discovered Lagrange and Gauss as a method of calculating elliptic integrals. This classical approach is limited to cases where the elliptic curve is given by a cubic equation with three real roots. We define an arithmetic-geometric mean for all elliptic curves over \mathbb{C} and detail the choices implicit in the classical construction.

Mathematics Subject Classification (2000). Primary 14H52; Secondary 14Q05.

Keywords. Arithmetic-Geometric Mean, Theta functions.

1. Introduction

The arithmetic-geometric mean (AGM), which will be reviewed in §2, is an algorithm devised by Gauss [6, III] that produces two sequences of real numbers, given the first terms, which converge quadratically to a common limit. The AGM has a geometric interpretation for an elliptic curve associated to the first terms of the sequences, giving a method for computing elliptic integrals (see [7], [3]). Recently, [8] gave a construction that produces the algebraic equations of this sequence of elliptic curves; this construction will be reviewed and expanded in §6. It is not obvious how to relate the points of period 2 and the limiting value with each choice of root when the sequences are not real (the concept of good sequences will be reviewed in §3), as the author of this note realized while studying the AGM for elliptic curves with complex multiplication. The main result in this paper identifies the various AGM's of a given E , for all the normalizations of its algebraic equation, as well as the period 2 points to which they correspond.

Theorem 1.1. *Let E_0/\mathbb{C} be an elliptic curve $y_0^2 = x_0(x_0 + a_0^2)(x_0 + b_0^2)$ isomorphic to a torus $\mathbb{C}/(\tau\mathbb{Z} + \mathbb{Z})$ for $\tau \in F$, where F is the fundamental domain for $\Gamma_2(4)$. Then for all $\gamma \in SL_2(\mathbb{Z})$ we get a different AGM depending as*

1. $\gamma \in \{\pm 1\}\Gamma_2(4)$: all good sequences for a_0 and b_0 , corresponding to $\{\gamma\tau, 1\} \mapsto \{2\gamma\tau, 1\}$
2. $\gamma \in \{\pm 1\} \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \Gamma_2(4)$: all good sequences for a_0 and $-b_0$, corresponding to $\{\gamma\tau, 1\} \mapsto \{2\gamma\tau, 1\}$
3. $\gamma \in \{\pm 1\} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \Gamma_2(4)$: all good sequences for $\sqrt{a_0^2 - b_0^2}$ and a_0 , corresponding to $\{[\gamma]\tau, 1\} \mapsto \{\frac{[\gamma]\tau}{2}, 1\}$
4. $\gamma \in \{\pm 1\} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \Gamma_2(4)$: all good sequences for $-\sqrt{a_0^2 - b_0^2}$ and a_0 , corresponding to $\{[\gamma]\tau, 1\} \mapsto \{\frac{[\gamma]\tau}{2}, 1\}$
5. $\gamma \in \{\pm 1\} \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix} \Gamma_2(4)$: all good sequences for b_0 and $\sqrt{b_0^2 - a_0^2}$, corresponding to $\{[\gamma]\tau, 1\} \mapsto \{\frac{1+[\gamma]\tau}{2}, 1\}$
6. $\gamma \in \{\pm 1\} \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \Gamma_2(4)$: all good sequences for b_0 and $-\sqrt{b_0^2 - a_0^2}$, corresponding to $\{[\gamma]\tau, 1\} \mapsto \{\frac{1+[\gamma]\tau}{2}, 1\}$

where $[\gamma]$ is the $\Gamma_2(4)$ component of γ .

2. Gauss's AGM

Let $a_0, b_0 \in \mathbb{R}$, $a_0, b_0 \geq 0$. The arithmetic-geometric mean (AGM) of a_0 and b_0 , denoted $M(a_0, b_0)$, is the common limit of the sequences $\{a_n\}_{n=0}^\infty$ and $\{b_n\}_{n=0}^\infty$ where $a_{n+1} = (a_n + b_n)/2$ and $b_{n+1} = \sqrt{a_n b_n}$. Assume $|a_0| > |b_0| > 0$ and consider the elliptic curve

$$E_0 : y_0^2 = x_0(x_0 + a_0^2)(x_0 + b_0^2).$$

The AGM of E_0 is defined to be the curve

$$E_1 : y_1^2 = x_1(x_1 + a_1^2)(x_1 + b_1^2),$$

with $a_1 = (a_0 + b_0)/2$ and $b_1 = \sqrt{a_0 b_0}$. As is well-known, E_0 is isomorphic to a torus $\mathbb{C}/(\tau\mathbb{Z} + \mathbb{Z})$, where $\tau \in \mathfrak{H}$, and $E_1 \simeq \mathbb{C}/(2\tau\mathbb{Z} + \mathbb{Z})$. Using these isomorphisms and the natural map $\mathbb{C}/(\tau\mathbb{Z} + \mathbb{Z}) \rightarrow \mathbb{C}/(2\tau\mathbb{Z} + \mathbb{Z})$ it is easy to show that $dx_0/y_0 = dx_1/y_1$. Combined with the quadratic convergence of the AGM, this fact was then classically very important to the study of elliptic integrals.

Theorem 2.1. [3] *Let a_0, b_0 be as above. Then*

$$\int_0^\infty \frac{dx_0}{\sqrt{x_0(x_0 + a_0^2)(x_0 + b_0^2)}} = \int_0^\infty \frac{dx}{\sqrt{x(x + M(a_0, b_0)^2)}} = \frac{\pi}{2M(a_0, b_0)}$$

where $E_\infty : y^2 = x(x + M(a_0, b_0)^2)^2$ is the limit of the sequence of elliptic curves.

3. The Complex Case

Let $a_0, b_0 \in \mathbb{C}$. There are two choices for b_1 . To avoid trivial cases, assume that $a_0, b_0 \in \mathbb{C}^\times$ with $a_0 \neq \pm b_0$. We extract the key ideas from [4, §2] to understand the complex AGM.

Definition 3.1. A square root b_1 of a_0b_0 is called the right choice if $|a_1 - b_1| \leq |a_1 + b_1|$ and, in the case of equality, $\text{Im}(\frac{b_1}{a_1}) > 0$.

Definition 3.2. A pair of sequences $\{a_n\}_{n=0}^\infty$ and $\{b_n\}_{n=0}^\infty$ is called good if b_{n+1} is the right choice for all but finitely many $n \geq 0$.

Proposition 3.3. [4, pg. 285-287] *Any pair of sequences $\{a_n\}_{n=0}^\infty$ and $\{b_n\}_{n=0}^\infty$ converge to a common limit, and this limit is nonzero iff they are good sequences.*

Remark 3.4. Thus all bad sequences have a limit of zero, which, as we will see, corresponds to a singular limiting curve, given by $y^2 = x^3$.

Definition 3.5. $\mu \in \mathbb{C}^\times$ is a value of the arithmetic-geometric mean, $M(a_0, b_0)$ if there are good sequences $\{a_n\}_{n=0}^\infty$ and $\{b_n\}_{n=0}^\infty$ such that $\mu = \lim_{n \rightarrow \infty} a_n = \lim_{n \rightarrow \infty} b_n$. If b_{n+1} is the right choice for all $n \geq 0$, then the common limit is called the simplest value of $M(a_0, b_0)$.

We now use theta functions to enumerate the limits for the complex AGM. Let $\tau \in \mathfrak{H}$, $q = e^{\pi i \tau}$. The Jacobi theta functions: $\theta_{00}(\tau) = \sum_{n=-\infty}^\infty q^{n^2}$, $\theta_{01}(\tau) = \sum_{n=-\infty}^\infty (-1)^n q^{n^2}$ and $\theta_{10}(\tau) = \sum_{n=-\infty}^\infty q^{(n+\frac{1}{2})^2}$ are well-known analytic functions. The following identities relate the theta functions to the AGM [2, Chap 2.1]: $\theta_{00}^2(2\tau) = \theta_{00}^2(\tau) + \theta_{01}^2(\tau)$, $\theta_{01}^2(2\tau) = \theta_{00}(\tau)\theta_{01}(\tau)$.

Lemma 3.6. [4, pg. 289-290] *Define $k'(\tau) = \theta_{01}^2(\tau)/\theta_{00}^2(\tau)$. Suppose there is a $\tau \in \mathfrak{H}$ such that $k'(\tau) = b_0/a_0$. Set $\mu = a_0/\theta_{00}^2(\tau)$ and, for $n \geq 0$, $a_n = \mu\theta_{00}^2(2^n\tau)$ and $b_n = \mu\theta_{01}^2(2^n\tau)$. Then (a) $\{a_n\}_{n=0}^\infty$ and $\{b_n\}_{n=0}^\infty$ are good sequences, and (b) $\lim a_n = \lim b_n = \mu$.*

Let

$$\begin{aligned} \Gamma(2)_0 &= \{\gamma \in \Gamma(2) : a \equiv d \equiv 1 \pmod{4}\} \\ \Gamma_2(4) &= \{\gamma \in \Gamma(2)_0 : c \equiv 0 \pmod{4}\}. \end{aligned}$$

It will be useful to note that $\Gamma(2) = \{\pm 1\} \cdot \Gamma(2)_0$ and $[\Gamma(2)_0 : \Gamma_2(4)] = 2$. The key to understanding the complex AGM is then the following.

Theorem 3.7. [4, §2] *$\theta_{00}^2(0, \tau)$ and $\theta_{01}^2(0, \tau)$ are modular forms of weight 1 for $\Gamma(2)_0$ and $\Gamma_2(4)$ respectively, with*

$$F = \{\tau \in \mathcal{H} : |\Re(\tau)| \leq 1, |\tau \pm 1/4| \geq 1/4, |\tau \pm 3/4| \geq 1/4\}$$

the fundamental domain for $\Gamma_2(4)$ after proper boundary identifications.

Corollary 3.8. [4, /S 2] *For all $a_0, b_0 \in \mathbb{C}^\times$ with $a_0 \neq \pm b_0$, there exists a $\tau \in F$ such that $k'(\tau) = b_0/a_0$.*

Lemma 3.9. [4, Lemma 2.9] *Let $a_0, b_0 \in \mathbb{C}^\times$ with $a_0 \neq \pm b_0$, $\tau \in \mathcal{H}$ and $k'(\tau) = b_0/a_0$. If $\tau \in F$ then $\mu = a_0/\theta_{00}^2(\tau)$ is the simplest value for $M(a_0, b_0)$, and the set of values for $M(a_0, b_0)$ is $\{a_0/\theta_{00}^2(\gamma\tau_0) : \gamma \in \Gamma_2(4)\}$.*

Remark 3.10. Thus all good AGM sequences for a pair of complex numbers are values of the same theta function evaluated at different τ 's, giving isomorphic tori.

4. Connections between algebraic equations for E/\mathbb{C}

We begin with an elliptic curve E/\mathbb{C} in (nonhomogeneous) Weierstrass form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with basepoint $\mathcal{O} = (0 : 1 : 0)$ and $a_1, \dots, a_6 \in \mathbb{C}$. As this is not of the form required for the classical AGM, $y^2 = x(x+a^2)(x+b^2)$, we put the curve E in Legendre form, $y^2 = x(x-1)(x-\lambda)$, where $\lambda = (e_1 - e_3)/(e_1 - e_2)$ for e_1, e_2, e_3 the roots of the cubic equation for E . As we will see, then the classical AGM applies with $a_0^2 = 1$ and $b_0^2 = \lambda$.

Remark 4.1. It is not guaranteed that λ is in \mathbb{R} , only that $\lambda \in \mathbb{C}$. Thus we must address the choice of the square root for b_1 in the complex case, this will be done in §5. For now, it is sufficient to note that either choice gives the same AGM E_1 .

In the following, we will study how the AGM for the Legendre form of E/\mathbb{C} relates to the classical case where we are given $y^2 = x(x+a^2)(x+b^2)$. We will begin to look at how the 6 isomorphic choices of λ affect the AGM, with the completion of this study appearing in §5. Finally, since E/\mathbb{C} , we will define an AGM for the elliptic curve in the form $y^2 = 4x^3 - g_2x - g_3$, which will be useful for defining correspondences between the algebraic and analytic interpretations of the AGM.

The key observation comes from the real and complex AGM's. Recall that $M(a, b)$ denotes the AGM of $a \neq b \in \mathbb{C}^\times$. It is an easily verifiable fact that for $a, b, c \in \mathbb{C}^\times$, $M(ca, cb) = cM(a, b)$, leading to the following.

Theorem 4.2. *Let $a_0, b_0, c \in \mathbb{C}^\times$, then*

$$\begin{aligned} E_0 : y_0^2 &= x_0(x_0 + a_0^2)(x_0 + b_0^2) \\ E'_0 : y_0'^2 &= x_0'(x_0' + c^2a_0^2)(x_0' + c^2b_0^2) \end{aligned}$$

are isomorphic, as are their respective AGM's

$$\begin{aligned} E_1 : y_1^2 &= x_1(x_1 + a_1^2)(x_1 + b_1^2) \\ E'_1 : y_1'^2 &= x_1'(x_1' + c^2a_1^2)(x_1' + c^2b_1^2). \end{aligned}$$

Lemma 4.3. [10, III.1] *Let E be an elliptic curve in Weierstrass form. Then any transformation of E of the form*

$$x = u^2x' + r \quad y = u^3y' + u^2sx' + t$$

with $u, r, s, t \in \mathbb{C}$, $u \neq 0$ yields an isomorphic elliptic curve E' , also in Weierstrass form with basepoint $\mathcal{O} = (0 : 1 : 0)$.

Proof of Theorem 4.2. Let E_0 and E'_0 be as above. Then the transformation $x'_0 = c^2x_0$, $y'_0 = c^3y_0$ is an isomorphism $E_0 \simeq E'_0$ by Lemma 4.3. As we saw above, the AGM of E_0 is $E_1 : y_1^2 = x_1(x_1 + a_1^2)(x_1 + b_1^2)$. Similarly for E'_0 , let $a'_0 = ca_0$ and $b'_0 = cb_0$, so that $a'_1 = (a'_0 + b'_0)/2 = ca_1$ and $b'_1 = \sqrt{a'_0b'_0} = cb_1$ and the AGM is $E'_1 : y_1'^2 = x_1'(x_1' + c^2a_1^2)(x_1' + c^2b_1^2)$. Then the transformation $x'_1 = c^2x_1$, $y'_1 = c^3y_1$ gives the desired isomorphism $E_1 \simeq E'_1$ by Lemma 4.3. \square

Corollary 4.4. *Let E_0 be an elliptic curve as above. Then the Legendre form of the curve E_0 with $\lambda = a_0^2/b_0^2$ gives an isomorphic AGM.*

Proof. Apply Theorem 4.2 with $c^2 = -1/b_0$. \square

Corollary 4.5. *Let $\mu \in \mathbb{C}^\times$. The elliptic curves*

$$\begin{aligned} E_0 : y_0^2 &= x_0(x_0 - 1)(x_0 - \mu) \\ E'_0 : y_0'^2 &= x'_0(x'_0 - 1)(x'_0 - 1/\mu) \end{aligned}$$

are isomorphic and have isomorphic AGM's.

Proof. Apply Theorem 4.2 with $c^2 = 1/\mu$. \square

In general, for each elliptic curve there are 6 isomorphic Legendre forms for that curve given by $y^2 = x(x-1)(x-\mu)$ where

$$\mu \in \left\{ \lambda, \frac{1}{\lambda}, 1-\lambda, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda-1}, \frac{\lambda-1}{\lambda} \right\}.$$

Given Corollary 4.5 we only need to consider 3 of these for each elliptic curve when calculating its possible AGM's.

Remark 4.6. In the case of $E_0 : y_0^2 = x_0(x_0 + a_0^2)(x_0 + b_0^2)$ we have $\lambda = \frac{0+a_0^2}{0+b_0^2}$. Then

$$1 - \lambda = 1 - \frac{a_0^2}{b_0^2} = \frac{b_0^2 - a_0^2}{b_0^2}$$

and Theorem 4.2 (with $c^2 = b_0^2$) means that the AGM for $y^2 = x(x-1)(x-(1-\lambda))$ is isomorphic to that for $y^2 = x(x-b_0^2)(x-(b_0^2-a_0^2))$. Similarly for $\frac{\lambda}{\lambda-1}$ and $y^2 = x(x-a_0^2)(x-(a_0^2-b_0^2))$.

Alternatively, it is also common to write E/\mathbb{C} in the form $E : y^2 = 4x^3 - g_2x - g_3$. Suppose we have an elliptic curve E'_0/\mathbb{C} ,

$$E'_0 : y_0'^2 = 4(x'_0 - e_{1,0})(x'_0 - e_{2,0})(x'_0 - e_{3,0}),$$

with the $e_{i,0}$'s distinct and $e_{1,0} + e_{2,0} + e_{3,0} = 0$. Following [3], we define an AGM for E'_0 using an isomorphism to an elliptic curve E_0 in the form above.

Proposition 4.7. *Let $E'_0 : y_0'^2 = 4(x'_0 - e_{1,0})(x'_0 - e_{2,0})(x'_0 - e_{3,0})$. Let $a_0 = \sqrt{e_{1,0} - e_{3,0}}$ and $b_0 = \sqrt{e_{1,0} - e_{2,0}}$. Then $E_0 : y_0^2 = x_0(x_0 + a_0^2)(x_0 + b_0^2)$ is isomorphic to E'_0 .*

Proof. Transform E'_0 into Weierstrass form, and apply Lemma 4.3. \square

As we saw above, the AGM for $E_0 : y_0^2 = x_0(x_0 + a_0^2)(x_0 + b_0^2)$ is the curve $E_1 : y_1^2 = x_1(x_1 + a_1^2)(x_1 + b_1^2)$ where a_1 and b_1 are the arithmetic and geometric means of a_0 and b_0 . With $a_0 = \sqrt{e_{1,0} - e_{3,0}}$ and $b_0 = \sqrt{e_{1,0} - e_{2,0}}$, we find that

$$e_{1,0} = (a_0^2 + b_0^2)/3, \quad e_{2,0} = (a_0^2 - 2b_0^2)/3, \quad e_{3,0} = (b_0^2 - 2a_0^2)/3.$$

We can then define

$$e_{1,1} = (a_1^2 + b_1^2)/3, \quad e_{2,1} = (a_1^2 - 2b_1^2)/3, \quad e_{3,1} = (b_1^2 - 2a_1^2)/3,$$

satisfying $a_1 = \sqrt{e_{1,1} - e_{3,1}}$, $b_1 = \sqrt{e_{1,1} - e_{2,1}}$ and $e_{1,1} + e_{2,1} + e_{3,1} = 0$.

Let $E'_1 : y_1'^2 = 4(x'_1 - e_{1,1})(x'_1 - e_{2,1})(x'_1 - e_{3,1})$. Then, using Proposition 4.7, we have an isomorphism $E'_1 \rightarrow E_1$. Thus we have the following result.

Proposition 4.8. *Let E'_0 be defined as above, then its AGM is $E'_1 : y_1'^2 = 4(x_1' - e_{1,1})(x_1' - e_{2,1})(x_1' - e_{3,1})$, where*

$$\begin{aligned} e_{1,1} &= \frac{e_{1,0}}{4} + \frac{1}{2}\sqrt{(e_{1,0} - e_{3,0})(e_{1,0} - e_{2,0})} \\ e_{2,1} &= \frac{e_{1,0}}{4} - \frac{1}{2}\sqrt{(e_{1,0} - e_{3,0})(e_{1,0} - e_{2,0})} \\ e_{3,1} &= -\frac{e_{1,0}}{2} \end{aligned}$$

5. The analytic interpretation of the AGM

In the classical case above, the AGM was defined analytically by $\mathbb{C}/(\tau\mathbb{Z} + \mathbb{Z}) \rightarrow \mathbb{C}/(2\tau\mathbb{Z} + \mathbb{Z})$. We will show how this corresponds to the complex AGM, and leads to the AGM for a cubic curve. With these correspondences, we will study how the choices of b_i and of λ in the Legendre form of E_0 affect the AGM.

Let the elliptic curve E/\mathbb{C} be written in the form

$$y^2 = 4x^3 - g_2x - g_3 = 4(x - e_1)(x - e_2)(x - e_3)$$

with the e_i 's distinct, $e_1 + e_2 + e_3 = 0$ and $e_1 > e_2 > e_3$, if the e_i 's are all real, $e_1 = \bar{e}_2$ and $e_3 \in \mathbb{R}$ otherwise. There is a lattice $\Lambda = \omega_2\mathbb{Z} + \omega_1\mathbb{Z}$, $\omega_2, \omega_1 \in \mathfrak{H}$ such that we can define a complex isomorphism of complex Lie Groups ([3], [10, VI.3]): $u : \mathbb{C}/\Lambda \rightarrow E/\mathbb{C}$ given by

$$u(z) = \begin{cases} (\wp(z; \omega_2, \omega_1), \wp'(z; \omega_2, \omega_1)) & z \notin \Lambda \\ (0 : 1 : 0) & z \in \Lambda \end{cases}$$

This map gives the following identifications among the points of order 2 of the torus and the elliptic curve:

$$(e_1, 0) = u(\omega_1/2) \quad (e_2, 0) = u((\omega_1 + \omega_2)/2) \quad (e_3, 0) = u(\omega_2/2).$$

Let $\tau = \omega_2/\omega_1 \in \mathcal{H}$. There is a holomorphic group isomorphism between the complex tori $\Lambda = \mathbb{C}/(\omega_2\mathbb{Z} + \omega_1\mathbb{Z})$ and $\Lambda_\tau = \mathbb{C}/(\tau\mathbb{Z} + \mathbb{Z})$ [5, 1.3]. As follows from the series definition of the Weierstrass \wp -function, $\tilde{\wp}(z) = \omega_1^2\wp(\omega_1 z)$, where $\tilde{\wp}(z)$ and $\wp(z)$ are associated to Λ and Λ_τ respectively. Then the map u above now gives

$$\begin{aligned} \omega_1^2 e_1 &= \omega_1^2 \wp(\omega_1/2) = \tilde{\wp}(1/2) \\ \omega_1^2 e_2 &= \omega_1^2 \wp(\omega_1/2 + \omega_2/2) = \tilde{\wp}(1/2 + \tau/2) \\ \omega_1^2 e_3 &= \omega_1^2 \wp(\omega_2/2) = \tilde{\wp}(\tau/2), \end{aligned}$$

completing the connection between the elliptic curve and the torus.

We wish to connect the torus with the complex case of the AGM, to better define and understand an AGM on the torus. Identities connecting theta functions and Weierstrass's \wp -function [9, pg 26 and 64], lead to the relations $\omega_1\sqrt{e_1 - e_3} = \pi\theta_{00}^2(\tau)$ and $\omega_1\sqrt{e_1 - e_2} = \pi\theta_{01}^2(\tau)$. Hence it makes sense to define an AGM by

$$\mathbb{C}/(\tau\mathbb{Z} + \mathbb{Z}) \xrightarrow{AGM} \mathbb{C}/(\tau\mathbb{Z} + \frac{1}{2}\mathbb{Z}).$$

Thus the AGM is obtained by moding out by $1/2 \in \mathbb{C}/(\tau\mathbb{Z} + \mathbb{Z})[2]$, which corresponds to $\omega_1/2 \in \mathbb{C}/(\omega_2\mathbb{Z} + \omega_1\mathbb{Z})$ and maps to e_1 under u .

Remark 5.1. This AGM corresponds to the theta function description of the complex case, $\theta_{00}^2(2\tau) = \theta_{00}^2(\tau) + \theta_{01}^2(\tau)$ and $\theta_{01}^2(2\tau) = \theta_{00}(\tau)\theta_{01}(\tau)$, more clearly if we instead define the AGM as

$$\mathbb{C}/(\tau\mathbb{Z} + \mathbb{Z}) \longrightarrow \mathbb{C}/(2\tau\mathbb{Z} + \mathbb{Z}),$$

but $\mathbb{C}/(2\tau\mathbb{Z} + \mathbb{Z})$ and $\mathbb{C}/(\tau\mathbb{Z} + \frac{1}{2}\mathbb{Z})$ are related by a holomorphic group isomorphism, so it is convenient to use the 2-torsion description of the AGM.

Now let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$. Then $\begin{pmatrix} \tau' \\ 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \tau \\ 1 \end{pmatrix}$ generates a lattice $\tau'\mathbb{Z} + \mathbb{Z} = \tau\mathbb{Z} + \mathbb{Z}$. Also, $\wp(z; \tau, 1) = \wp(z; \tau', 1)$, so $\mathbb{C}/(\tau\mathbb{Z} + \mathbb{Z})$ and $\mathbb{C}/(\tau'\mathbb{Z} + \mathbb{Z})$ correspond to the same elliptic curve E/\mathbb{C} .

Definition 5.2. Let $\mathbb{C}/(\tau\mathbb{Z} + \mathbb{Z}) \xrightarrow{\sim} E/\mathbb{C} : y^2 = 4(x - e_1)(x - e_2)(x - e_3)$. Define a function $\lambda : \mathbb{C} \rightarrow \mathbb{C}$ by $\lambda(\tau) = \frac{e_1 - e_3}{e_1 - e_2}$.

Note that λ corresponds to the λ in the Legendre form of our elliptic curve above, hence the following shows the affect of varying the choice of λ on the AGM.

Proposition 5.3. [1, 7§3.4] For all $\delta \in \Gamma(2)$, $\lambda(\delta\tau) = \lambda(\tau)$.

Recall

$$SL_2(\mathbb{Z})/\Gamma(2) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \right\}.$$

Theorem 5.4. Let $\tau = \omega_2/\omega_1 \in \mathcal{H}$ and $\lambda(\tau) = (e_1 - e_3)/(e_1 - e_2)$. Let $\gamma \in SL_2(\mathbb{Z})/\Gamma(2)$, then $\lambda(\gamma\tau)$ is as below:

$$\begin{aligned} \lambda\left(\frac{1}{\tau}\right) &= \frac{\lambda(\tau)}{\lambda(\tau)-1}, & \lambda(1-\tau) &= \frac{1}{\lambda(\tau)}, & \lambda\left(\frac{1}{1-\tau}\right) &= \frac{1}{1-\lambda(\tau)}, \\ \lambda\left(\frac{\tau}{\tau-1}\right) &= 1 - \lambda(\tau), & \lambda\left(\frac{\tau-1}{\tau}\right) &= \frac{\lambda(\tau)-1}{\lambda(\tau)}. \end{aligned}$$

Proof. First we note that $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$ are generators for $SL_2(\mathbb{Z})/\Gamma(2)$, hence it sufficient to study $\lambda(\gamma\tau)$ for these two γ 's.

Case 1: $\gamma = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

We begin by noting that $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \tau \\ 1 \end{pmatrix} = \begin{pmatrix} 1/\tau \\ 1 \end{pmatrix}$ where $1/\tau = \omega_1/\omega_2$. Hence γ switches the roles of ω_1 and ω_2 , and thus also $u(\omega_1) = e_1$ and $u(\omega_2) = e_3$ ($\omega_1/2 + \omega_2/2$ and hence e_2 are fixed). This gives us

$$\lambda\left(\frac{1}{\tau}\right) = \frac{e_3 - e_1}{e_3 - e_2} = \frac{e_1 - e_3}{e_2 - e_3 + e_1 - e_1} = \frac{e_1 - e_3}{e_1 - e_2} \cdot \frac{e_1 - e_2}{(e_1 - e_3) - (e_1 - e_2)} = \frac{\lambda(\tau)}{\lambda(\tau) - 1}.$$

Case 2: $\gamma = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$

Similarly, since here γ is easily seen to switch the roles of e_2 and e_3 (e_1 is fixed), we find that $\lambda(1-\tau) = \frac{e_1 - e_2}{e_1 - e_3} = \frac{1}{\lambda(\tau)}$. \square

Corollary 5.5. Let $\gamma \in SL_2(\mathbb{Z})/\Gamma(2)$, and $\tau' = \gamma\tau$, then

$$\lambda(\tau') = \frac{e_i - e_k}{e_i - e_j}, \quad \{i, j, k\} = \{1, 2, 3\}$$

follows the transformations in Theorem 5.4. Then the AGM is given by moding out by $1/2 \leftrightarrow \omega'_1 \leftrightarrow e_i$, where $\gamma \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} \omega'_1 \\ \omega'_2 \end{pmatrix}$.

Recall that in the complex case we had, for $\tau_0 \in F$, the fundamental domain for $\Gamma_2(4)$, the set of values for $M(a, b) = \{a/\theta_{00}^2(\gamma\tau_0) : \gamma \in \Gamma_2(4)\}$. Thus different $\gamma \in \Gamma_2(4)$ generating lattices $\gamma\tau\mathbb{Z} + \mathbb{Z}$ giving isomorphic tori account for all of the possible good sequences.

However, $[\Gamma(2) : \Gamma_2(4)] = 4$, so it still remains to see how the $\gamma \in \Gamma(2)/\Gamma_2(4)$ affect the AGM. We saw above that $\Gamma(2) = \{\pm 1\} \cdot \Gamma(2)_0$, where $-I\tau = \tau$. Thus we only need to understand the affect of elements of $\Gamma(2)_0/\Gamma_2(4)$, where $[\Gamma(2)_0 : \Gamma_2(4)] = 2$. This group is represented by $\{(\frac{1}{0} \ 0), (\frac{1}{2} \ 1)\}$ in $\Gamma(4)$ where, for $k'(\tau) = \theta_{01}^2(\tau)/\theta_{00}^2(\tau)$, we have $k'((\frac{1}{2} \ 1)\tau) = -k'(\tau)$. Thus acting by $(\frac{1}{2} \ 1)$ corresponds to taking the AGM with a_0 and $-b_0$ (or $-a_0$ and b_0), instead of a_0 and b_0 . This proves Theorem 1.1.

6. The Chord Construction

In this section we look at Lehavi and Livne's chord construction [8]. This formulation of the AGM explicitly shows (without appealing to the analytic interpretation) that this process is moding out by a 2-torsion point.

Let $E_0 \subset \mathbb{P}^2(\mathbb{C})$ be an elliptic curve with $E_0[2] = \{\mathcal{O}, \alpha, \beta, \gamma = \alpha + \beta\}$, where $\mathcal{O} = [0 : 1 : 0]$ is the basepoint. We need to identify, say, p and $p + \alpha$ for all $p \in E_0$. We accomplish this by moving to the dual space \mathbb{P}^{2*} , where the AGM $E_1 = E_0/\alpha \subset \mathbb{P}^{2*}$ is the curve given by the images of the lines through points p and $p + \alpha$. This is the chord construction.

Theorem 6.1. [8, Theorem 3] *The chord construction is an embedding.*

Let us look at this construction more explicitly. Denote homogeneous coordinates for \mathbb{P}^2 and \mathbb{P}^{2*} by $[X : Y : Z]$ and $[U : V : W]$, respectively. As usual, define affine coordinates $x := X/Z$ and $y := Y/Z$. Inhomogeneously, our elliptic curve E_0/\mathbb{C} will be given by a Weierstrass equation of the form

$$E_0 : y^2 = x(x + a_0^2)(x + b_0^2) = x^3 + (a_0^2 + b_0^2)x^2 + a_0^2b_0^2x,$$

as in the classical formulation of the AGM. Thus the points of order 2 on E_0 are $E_0[2] = \{\mathcal{O}, (0, 0), (-a_0^2, 0), (-b_0^2, 0)\}$.

For ease of notation, we first consider the chord construction for the point of order 2, $(0, 0)$. Let $p = (x(p), y(p)) \in E_0$. Then $p + (0, 0)$ is given by

$$x(p + (0, 0)) = \frac{a_0^2b_0^2}{x(p)} \quad y(p + (0, 0)) = \frac{-a_0^2b_0^2y(p)}{x(p)^2}$$

by addition on the elliptic curve E_0 [10, §III.2].

Lemma 6.2. [8, Lemma 8] *Let $p = (x(p), y(p)) \in E_0$. Then the lines of the chord construction give points*

$$[y(p)(x(p)^2 + a_0^2b_0^2) : a_0^2b_0^2x(p) - x(p)^3 : -2a_0^2b_0^2x(p)y(p)] \in \mathbb{P}^{2*}.$$

Proof. Denote the line through p and $p + (0, 0)$ by $y = mx + b$. Then

$$m = \frac{y(p) - y(p + (0, 0))}{x(p) - x(p + (0, 0))} = \frac{y(p) + a_0^2b_0^2y(p)/x(p)}{x(p) - a_0^2b_0^2/x(p)} = \frac{y(p)(x(p) + a_0^2b_0^2)}{x(p)^3 - a_0^2b_0^2x(p)}$$

and

$$b = y(p) - mx(p) = \frac{-2a_0^2 b_0^2 x(p)y(p)}{x(p)^3 - a_0^2 b_0^2 x(p)}.$$

When mapping to the dual coordinates, a line $y = mx + b$, denoted by $[m : l : b]_L$, goes to the point $[m : -1 : b]$. Simplifying the formulas above for $[m : -1 : b]$ we get the result. \square

We wish to identify the curve $E_1 = E_0/(0,0)$. We first note that the dual of the line $y = 0 \subset \mathbb{P}^2$ is the point $[0 : 1 : 0]$ and vice versa. Hence $E_1[2] \subset V = 0$. There are three values of $x(p)$ which give $V = 0$: $0, \pm a_0 b_0$. Substituting these values into the coordinates above we get (after simplification) $[1 : 0 : 0]$, $[1 : 0 : a_0 b_0]$, $[1 : 0 : -a_0 b_0]$.

Recall that $y = 0 \in \mathbb{P}^2 \mapsto [0 : 1 : 0] \in \mathbb{P}^{2*}$, hence the tangent to the basepoint must come from the unique point $(\mu, 0)$ on $y = 0$ such that no other line of the chord construction goes through $(\mu, 0)$. The x -coordinate of the intersection of a chord and $y = 0$ is given by

$$\mu = -\frac{b}{m} = \frac{2a_0^2 b_0^2 x(p)y(p)}{y(p)(x(p)^2 + a_0^2 b_0^2)} = \frac{2a_0^2 b_0^2 x(p)}{x(p)^2 + a_0^2 b_0^2}.$$

Barring $(0,0)$, the intersections of E_0 and $y = 0$ are $(-a_0^2, 0)$ and $(-b_0^2, 0)$. Thus

$$\mu = -\frac{2a_0^2 b_0^2}{a_0^2 + b_0^2}.$$

The dual of the point $[\mu : 0 : 1] = [1 : 0 : \frac{1}{\mu}] \in \mathbb{P}^2$ is the line $U + \frac{1}{\mu}W = 0$. Hence, following the argument above, this line is the line at infinity for the curve E_1 . Using Lemma 6.2 we find that

$$\begin{aligned} & \frac{-8a_0^6 b_0^2}{(a_0^2 + b_0^2)^2 - 4a_0^2 b_0^2} V^2(U + \frac{1}{\mu}W) \\ &= W^3 + \frac{2\mu a_0^2 b_0^2}{\mu^2 - a_0^2 b_0^2} (U + \frac{1}{\mu}W)W^2 - \frac{\mu^2 a_0^2 b_0^2}{\mu^2 - a_0^2 b_0^2} (U + \frac{1}{\mu}W)^2 W \end{aligned}$$

where

$$\begin{aligned} & W^3 - a_0^2 b_0^2 (U - \frac{1}{\mu}W)^2 W \\ &= \left(\frac{4a_0^2 b_0^2 - (a_0^2 + b_0^2)^2}{4a_0^2 b_0^2} \right) \left(W^3 + \frac{2\mu a_0^2 b_0^2}{\mu^2 - a_0^2 b_0^2} U W^2 - \frac{\mu^2 a_0^2 b_0^2}{\mu^2 - a_0^2 b_0^2} U^2 W \right). \end{aligned}$$

Finally, let $v = V/(U + \frac{1}{\mu}W)$ and $w = W/(U + \frac{1}{\mu}W)$ be affine coordinates for \mathbb{P}^{2*} . Thus we have proven the following.

Theorem 6.3. *Let $E_0 : y^2 = x^3 + (a_0^2 + b_0^2)x^2 + a_0^2 b_0^2 x$ be an elliptic curve over \mathbb{C} . Then moding out by $(0,0) \in E_0[2]$ we get the curve*

$$E_1 : \frac{-8a_0^6 b_0^2}{(a_0^2 + b_0^2)^2 - 4a_0^2 b_0^2} v^2 = w^3 + \frac{2\mu a_0^2 b_0^2}{\mu^2 - a_0^2 b_0^2} w^2 - \frac{\mu^2 a_0^2 b_0^2}{\mu^2 - a_0^2 b_0^2} w.$$

Proposition 6.4. *Let E_0/\mathbb{C} be as above. Then E_1/\mathbb{C} given by the chord construction is isomorphic to the classical AGM for E_0 .*

Proof. We compare j -invariants. Both E_1 and the classical AGM for E_0 have

$$j = \frac{16(a_0^4 + 14a_0^2b_0^2 + b_0^4)^3}{a_0^2b_0^2(a_0^2 - b_0^2)^4}. \quad \square$$

Remark 6.5. Moding out by the 2-torsion point $(-a_0^2, 0)$ gives

$$\begin{aligned} [m : -1 : b] &= [y(p)(x(p)^2 + 2a_0^2x(p) - a_0^2b_0^2 + 2a_0^4) : \\ &\quad -(x(p) + a_0^2)(x(p)^2 + 2a_0^2x(p) + a_0^2b_0^2) : \\ &\quad a_0^2y(p)(x(p)^2 + 2b_0^2x(p) + a_0^2b_0^2)] \\ V^2(U + \frac{1}{\mu}W) &= \left(\frac{1}{a_0^4b_0^4 - a_0^6b_0^2}\right) \\ &\quad \cdot (W^3 + \frac{a_0^2(5b_0^2 - 4a_0^2)}{2(a_0^2 - b_0^2)}(U + \frac{1}{\mu}W)W^2 + \frac{2a_0^4b_0^2}{b_0^2 - a_0^2}(U + \frac{1}{\mu}W)^2W) \\ j &= \frac{16(16a_0^4 - 16a_0^2b_0^2 + b_0^4)^3}{a_0^2b_0^8(a_0^2 - b_0^2)} \end{aligned}$$

and similarly for $(-b_0^2, 0)$, with the roles of a_0 and b_0 reversed.

References

- [1] L. Ahlfors, *Complex Analysis. An introduction to the theory of analytic functions of one complex variable*. 3rd edition, McGraw-Hill Book Co., 1978.
- [2] J. A. Borwein and P. B. Borwein. *Pi and the AGM. A Study in Analytic Number Theory and Computational Complexity*. John Wiley & Sons, Inc., 1987.
- [3] 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.
- [4] D. Cox, *The arithmetic-geometric mean of Gauss*. *Enseign. Math. (2)* **32** (1985), 275–330.
- [5] F. Diamond and J. Shurman. *A First Course in Modular Forms*. Springer Science+Business Media, 2005.
- [6] C. F. Gauss. *Werke*. Göttingen-Leipzig, 1868-1927.
- [7] D. Grayson, *The arithogeometric mean*. *Arch. Math. (Basel)* **52** (1989), 507–512.
- [8] D. Lehavi and R. Livne. *The Chord Construction* arXiv:math/0110338v1 [math.AG].
- [9] D. Mumford, *Tata Lectures on Theta I*. Birkhäuser Boston, Inc., 1983.
- [10] Silverman, J. H. *The Arithmetic of Elliptic Curves*. Springer-Verlag, 1992.

Acknowledgment

The author would like to thank her advisor, Emma Previato, for introducing her to this problem and for her incredible help and guidance throughout this study.

Eleanor Farrington
 Department of Mathematics and Statistics
 Boston University
 Boston, MA 02215
 USA
 e-mail: efarring@bu.edu