

## Poster #94

### Abstract:

Gauss's arithmetic-geometric mean (AGM) for real numbers is the common limit of the recursively defined sequences of the arithmetic and geometric means of two real numbers. Finding the geometric mean requires a square root, leading to a non-obvious choice when the same process is applied to complex numbers. As it turns out, the "right" choice does not have to be made every time to lead to an interesting limit. The collection of interesting limits can be described using specific types of quasi-periodic functions (theta functions), which in turn leads to an interpretation of the AGM for elliptic curves over the complex numbers defined by cubic equations with all real roots. Our goal is to expand this interpretation to all elliptic curves over the complex numbers. We then consider applications of the elliptic curve AGM to calculating Pi and cryptography through point counting algorithms for elliptic curves.

## Introduction

Let  $a, b \in \mathbb{R}$ ,  $a, b \geq 0$ . The arithmetic-geometric mean of  $a$  and  $b$ , denoted  $M(a, b)$ , is the common limit of the sequences  $\{a_n\}_{n=0}^{\infty}$  and  $\{b_n\}_{n=0}^{\infty}$  where

$$\begin{aligned} a_0 &= a & b_0 &= b \\ a_{n+1} &= \frac{(a_n + b_n)}{2} & b_{n+1} &= \sqrt{a_n b_n} \end{aligned}$$

An elliptic curve  $E$  over  $\mathbb{C}$  is a non-singular cubic plane curve

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

on which is defined an addition of points (see illustration below) making it a group (a mathematical structure with the properties of associativity, inverses and containing an identity element).

Now assume  $|a_0| > |b_0| > 0$  and consider the elliptic curve

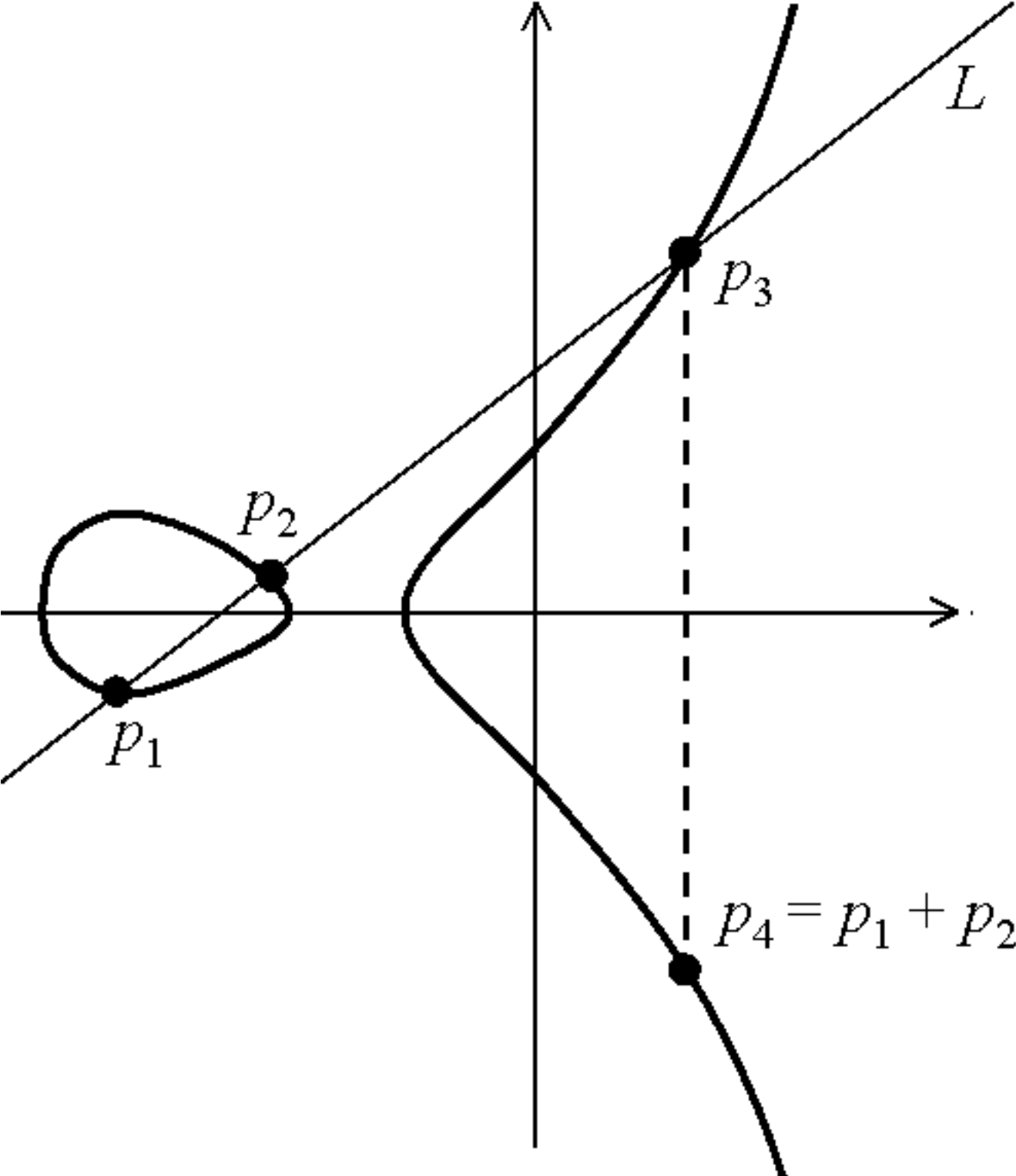
$$E_0 : y_0^2 = x_0(x_0 + a_0^2)(x_0 + b_0^2).$$

The elliptic curve AGM for  $E_0$  is defined to be the elliptic 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  $b_0$  [3], [8].

# Elliptic Curve Addition



From [9]

## The Complex AGM

Let  $a, b \in \mathbb{C}$ , then the choice of  $b_1$  is no longer obvious. To avoid trivial cases, let us assume that  $a, b \in \mathbb{C}^\times$  with  $a \neq \pm b$ . Following [4 §2] we make the following definition to distinguish the two choices for  $b_1$ .

**Definition 1.** A square root  $b_1$  of  $ab$  is called the *right choice* if  $|a_1 - b_1| \leq |a_1 + b_1|$  and, when we have equality,  $\text{Im}(\frac{b_1}{a_1}) > 0$ .

The unexpected thing is that it isn't necessary to always make the right choice to get an interesting sequence.

**Definition 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  $(a_n b_n)^{\frac{1}{2}}$  for all but finitely many  $n \geq 0$ .

**Proposition 1.** 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 if and only if they are good sequences.

## Theta Functions

Let  $\tau \in \mathfrak{H} = \{\tau \in \mathbb{C} \mid \Im(\tau) > 0\}$  and define  $q = e^{\pi i \tau}$ . The Jacobi theta functions are the following:

$$\theta_{00}(\tau) = 1 + \sum_{n=-\infty}^{\infty} q^{n^2}$$

$$\theta_{01}(\tau) = 1 + \sum_{n=-\infty}^{\infty} (-1)^n q^{n^2}$$

$$\theta_{10}(\tau) = \sum_{n=-\infty}^{\infty} q^{(n+\frac{1}{2})^2}$$

These are holomorphic functions of  $\tau$ , quasi-periodic with periods  $\tau$  and 1. They are important for our study of the AGM because of the following properties [2, Ch. 2.1]:

$$\begin{aligned}\theta_{00}^2(2\tau) &= \theta_{00}^2(\tau) + \theta_{01}^2(\tau) \\ \theta_{01}^2(2\tau) &= \theta_{00}(\tau)\theta_{01}(\tau).\end{aligned}$$

**Lemma 1** (4 §2). Define  $k'(\tau) = \theta_{01}^2(\tau)/\theta_{00}^2(\tau)$ . Suppose there is a  $\tau \in \mathfrak{H}$  such that  $k'(\tau) = b/a$ . Set  $\mu = a/\theta_{00}^2(\tau)$  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

- $\{a_n\}_{n=0}^{\infty}$  and  $\{b_n\}_{n=0}^{\infty}$  are good sequences
- $\lim a_n = \lim b_n = \mu$
- As we vary  $\tau \in \mathfrak{H}$  such that  $k'(\tau) = b/a$  we get all of the good sequences.

## Lattices and Tori

A lattice  $\Lambda$  in  $\mathbb{C}$  is a set of points with an  $\mathbb{R}$ -independent basis  $\omega_1$  and  $\omega_2$ ,  $\Lambda = \{m\omega_1 + n\omega_2 \mid m, n \in \mathbb{R}\}$ . Every such lattice is isomorphic to a lattice with basis 1 and  $\tau \in \mathfrak{H}$ . Let

$$SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(2, 2) \mid a, b, c, d \in \mathbb{Z}, \det = \pm 1 \right\}.$$

Then  $\Lambda = \Lambda'$  if and only if

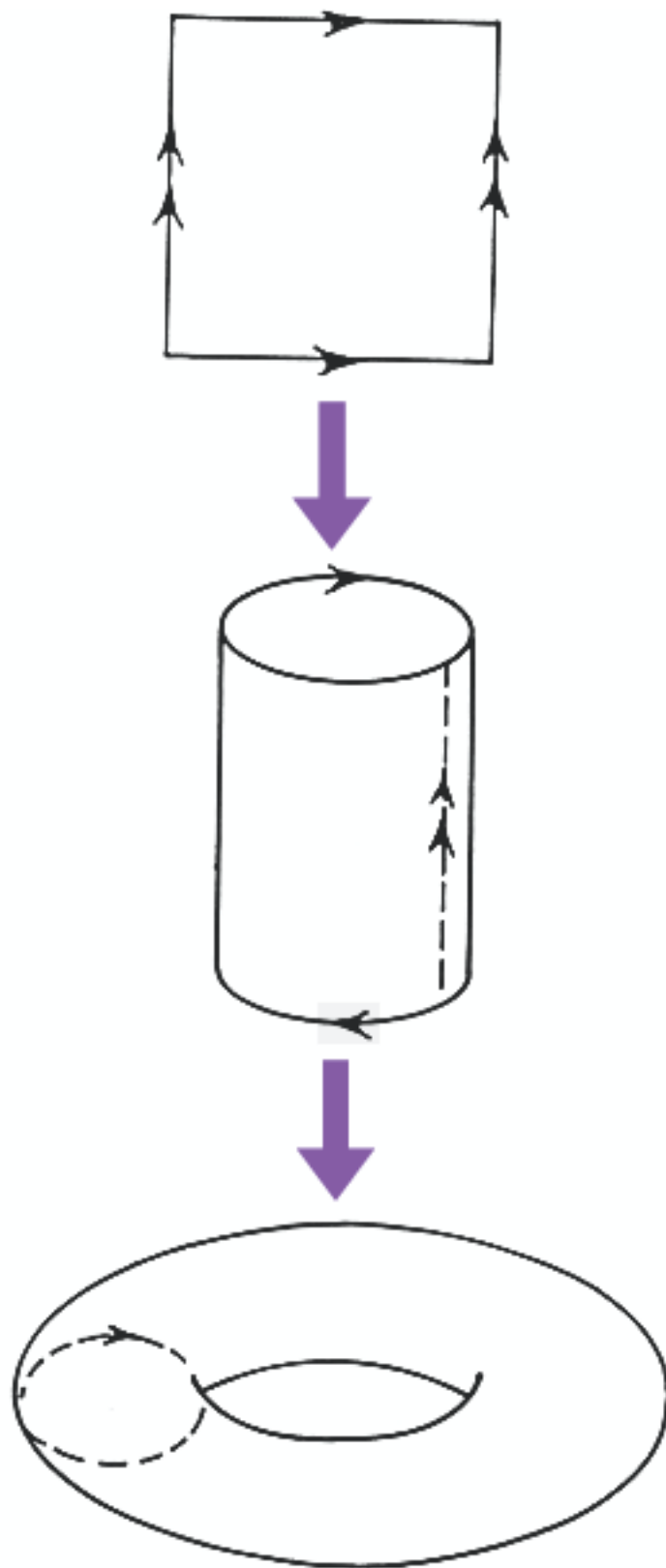
$$\begin{pmatrix} \omega'_2 \\ \omega'_1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_2 \\ \omega_1 \end{pmatrix}.$$

A complex torus is a quotient of the complex plane by a lattice,  $\mathbb{C}/\Lambda = \{z + \Lambda \mid z \in \mathbb{C}\}$ . Weierstrass's  $\wp$ -function is a special function which gives us isomorphisms between tori and elliptic curves [5 §1.3].

A few other useful matrix groups:

$$\begin{aligned} \Gamma(2) &= \{ \gamma \in SL_2(\mathbb{Z}) \mid \gamma \equiv I \pmod{2} \} \\ \Gamma(2)_0 &= \{ \gamma \in \Gamma(2) : a \equiv d \equiv 1 \pmod{4} \} \\ \Gamma_2(4) &= \{ \gamma \in \Gamma(2)_0 : c \equiv 0 \pmod{4} \}. \end{aligned}$$

# A Torus from $\mathbb{C}/\Lambda$



Images from [10]

## AGM's for Tori and Elliptic Curves

The complex AGM leads us to define the torus AGM. Recall the complex case in terms of theta functions essentially boiled down to  $\tau \rightarrow 2\tau$ . Define the AGM for a torus as

$$\mathbb{C}/(\tau\mathbb{Z} + \mathbb{Z}) \rightarrow \mathbb{C}/(2\tau\mathbb{Z} + \mathbb{Z}).$$

We can also express this as modding out by the point of order two  $\frac{1}{2} \in \mathbb{C}/(\tau\mathbb{Z} + \mathbb{Z})$  (i.e. setting  $z = z + 1/2$  for all  $z \in \mathbb{C}/(\tau\mathbb{Z} + \mathbb{Z})$  where  $1/2 + 1/2 = 0$ ).

Again, using the  $\wp$ -function, we can connect this AGM for a torus with an AGM for an elliptic curve, by the following diagram

$$\begin{array}{ccc} \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z}) & \xrightarrow{\sim} & E_\tau \\ \uparrow F & & \uparrow \varphi \\ \mathbb{C}/(\mathbb{Z} + 2\tau\mathbb{Z}) & \xrightarrow{\sim} & E_{2\tau} \end{array}$$

## The Main Results

**Definition 3.** Suppose we have  $\mathbb{C}/(\tau\mathbb{Z} + \mathbb{Z}) \xrightarrow{\sim} E/\mathbb{C} : y^2 = 4(x - e_1)(x - e_2)(x - e_3)$ . Define a function  $\lambda : \mathbb{C} \rightarrow \mathbb{C}$  by

$$\lambda(\tau) = \frac{e_1 - e_3}{e_1 - e_2}$$

**Proposition 2** (1 Ch. 7.3.4). *For all  $\delta \in \Gamma(2)$ ,  $\lambda(\delta\tau) = \lambda(\tau)$ .*

$SL_2(\mathbb{Z})/\Gamma(2)$  is

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \right\}$$

**Theorem 1.** *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:*

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

**Corollary 1.** *Let  $\gamma \in SL_2(\mathbb{Z})/\Gamma(2)$ , and  $\tau' = \gamma\tau$ , then*

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

obeys the transformations in Theorem 1. Then

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

is moding out by  $1/2 \leftrightarrow \omega'_1 \leftrightarrow e_i$ .

Thus varying  $\tau$  by an element of  $SL_2(\mathbb{Z})/\Gamma(2)$  changes which point of order 2 the torus AGM mods out by.

In the complex case, for  $\tau_0 \in F$ , the fundamental domain for  $\Gamma_2(4)$  the set of values for  $M(a, b)$  is

$$\{a/\theta_{00}^2(\gamma\tau_0) : \gamma \in \Gamma_2(4)\}.$$

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.

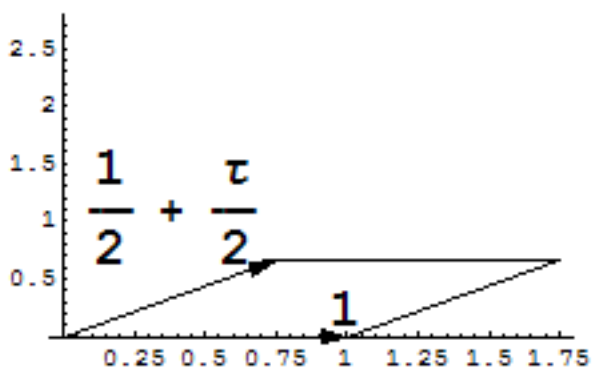
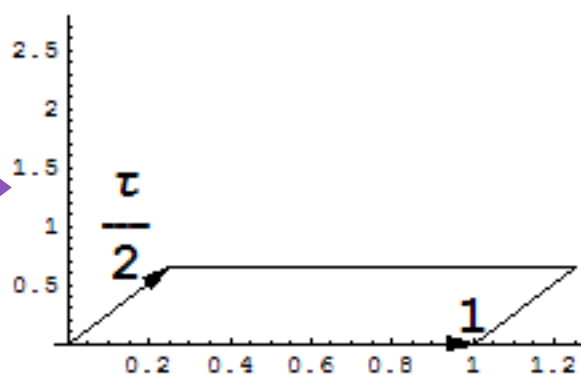
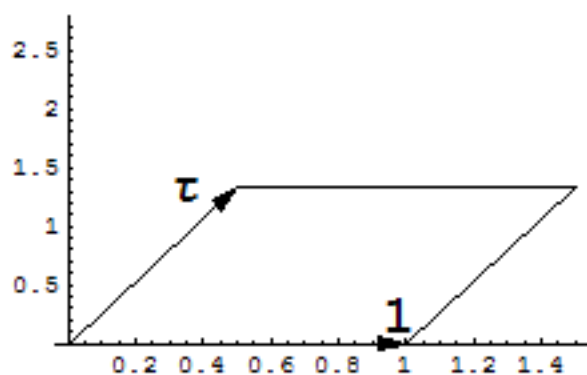
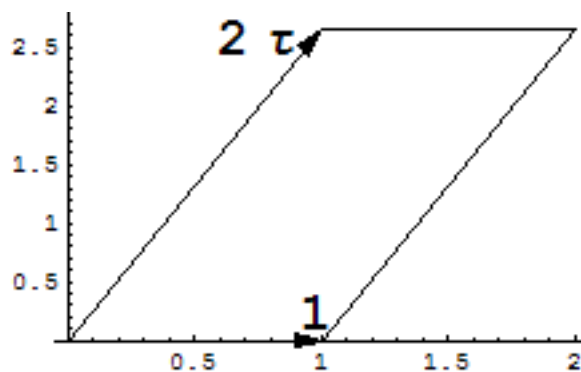
It still remains to see how the  $\gamma \in \Gamma(2)/\Gamma_2(4)$  effect the torus AGM.  $\Gamma(2) = \{\pm 1\} \cdot \Gamma(2)_0$ , where  $-I\tau = \tau$ . Finally the group  $\Gamma(2)_0/\Gamma_2(4)$ , represented by  $\left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}\right\}$ , in  $\Gamma(4)$  gives, for  $k'(\tau) = \theta_{01}^2(\tau)/\theta_{00}^2(\tau)$ ,

$$k'\left(\frac{\tau}{2\tau + 1}\right) = -k'(\tau).$$

Thus acting by  $\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$  corresponds to taking the AGM with  $a_0$  and  $-b_0$  (or  $-a_0$  and  $b_0$ ), instead of  $a_0$  and  $b_0$ .

## The Choice of Point of Order 2

Ex.  $\tau = \frac{1}{2} + \frac{\sqrt{-7}}{2}$



## Future Directions: A Genus 3 AGM

Associated to every compact Riemann surface,  $X$ , there is a higher dimensional analogue of a torus, called the Jacobian of  $X$ , or  $Jac(X)$ . Let  $L$  be a lattice in  $\mathbb{C}^g$  with  $2g$  generators (subject to some technical constraints), then

$$Jac(X) = \mathbb{C}^g / L.$$

Some special Jacobians can be broken up into a product of tori, eg. for  $g=3$

$$\mathbb{C}^3 / L = \mathbb{C} / \Lambda_1 \times \mathbb{C} / \Lambda_2 \times \mathbb{C} / \Lambda_3.$$

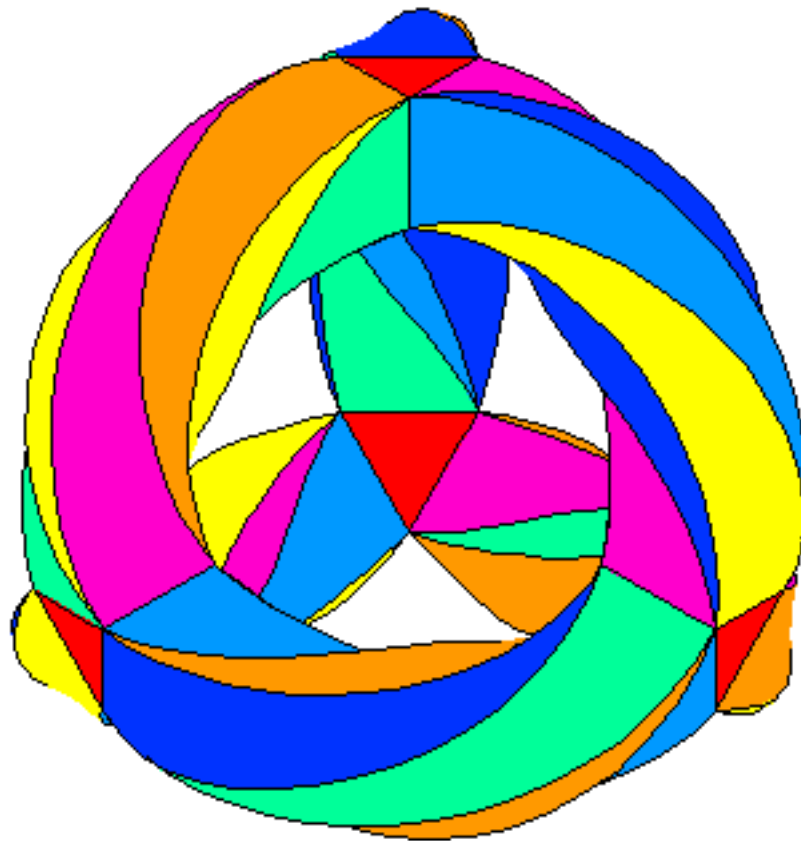
One such  $X$  is Klein's quartic curve,  $K$ , a genus 3 Riemann surface given by the equation

$$X^3Y + Y^3Z + Z^3X = 0$$

in  $\mathbb{P}^2(\mathbb{C})$ . Our goal is to define an AGM on  $K$  by applying the results detailed here for tori and elliptic curves to the tori in the product expansion of  $Jac(K)$ . We should then be able to generalize to all Jacobians which can be written as products of tori.

## Klein's Quartic Curve

$X^3Y + Y^3Z + Z^3X = 0$  triangular tiling embedded in  $\mathbb{R}^3$ :



From [6]

## Application: Calculating Pi

The elliptic curve AGM was first developed by Gauss and Lagrange as a method of calculating integrals of the form

$$\int_a^b \frac{dx}{\sqrt{P(x)}}$$

where  $P(x)$  is of degree 3 or 4, known as *elliptic integrals*. Let  $E_\tau$  be an elliptic curve with corresponding torus  $\mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$ . Recall we have the following diagram

$$\begin{array}{ccc} \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z}) & \xrightarrow{\sim} & E_\tau \\ \uparrow F & & \uparrow \varphi \\ \mathbb{C}/(\mathbb{Z} + 2\tau\mathbb{Z}) & \xrightarrow{\sim} & E_{2\tau} \end{array}$$

where  $F(z + \Lambda_{2\tau}) = z + \Lambda_\tau$ ,  $\mu_0 : \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z}) \rightarrow E_\tau$ ,  $\mu_1 : \mathbb{C}/(\mathbb{Z} + 2\tau\mathbb{Z}) \rightarrow E_{2\tau}$ , and  $\varphi$  is the degree 2 map such that the diagram commutes. Defining  $\varphi = \mu_0 \circ F \circ \mu_1^{-1}$ , it is not hard to show that  $\varphi^*(dx_0/y_0) = dx_1/y_1$ .

## Calculating Pi, cont'd.

Thus

$$\begin{aligned} \int_0^\infty \frac{dx_0}{\sqrt{x_0(x_0+a_0^2)(x_0+b_0^2)}} &= \int_0^\infty \frac{dx_0}{y_0} \\ &= \int_0^\infty \frac{dx_1}{y_1} = \int_0^\infty \frac{dx_1}{\sqrt{x_1(x_1+a_1^2)(x_1+b_1^2)}}. \end{aligned}$$

**Theorem 2 (3).** Let  $a_0, b_0 \in \mathbb{R}$ ,  $a_0, b_0 \geq 0$ .  
Then

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

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

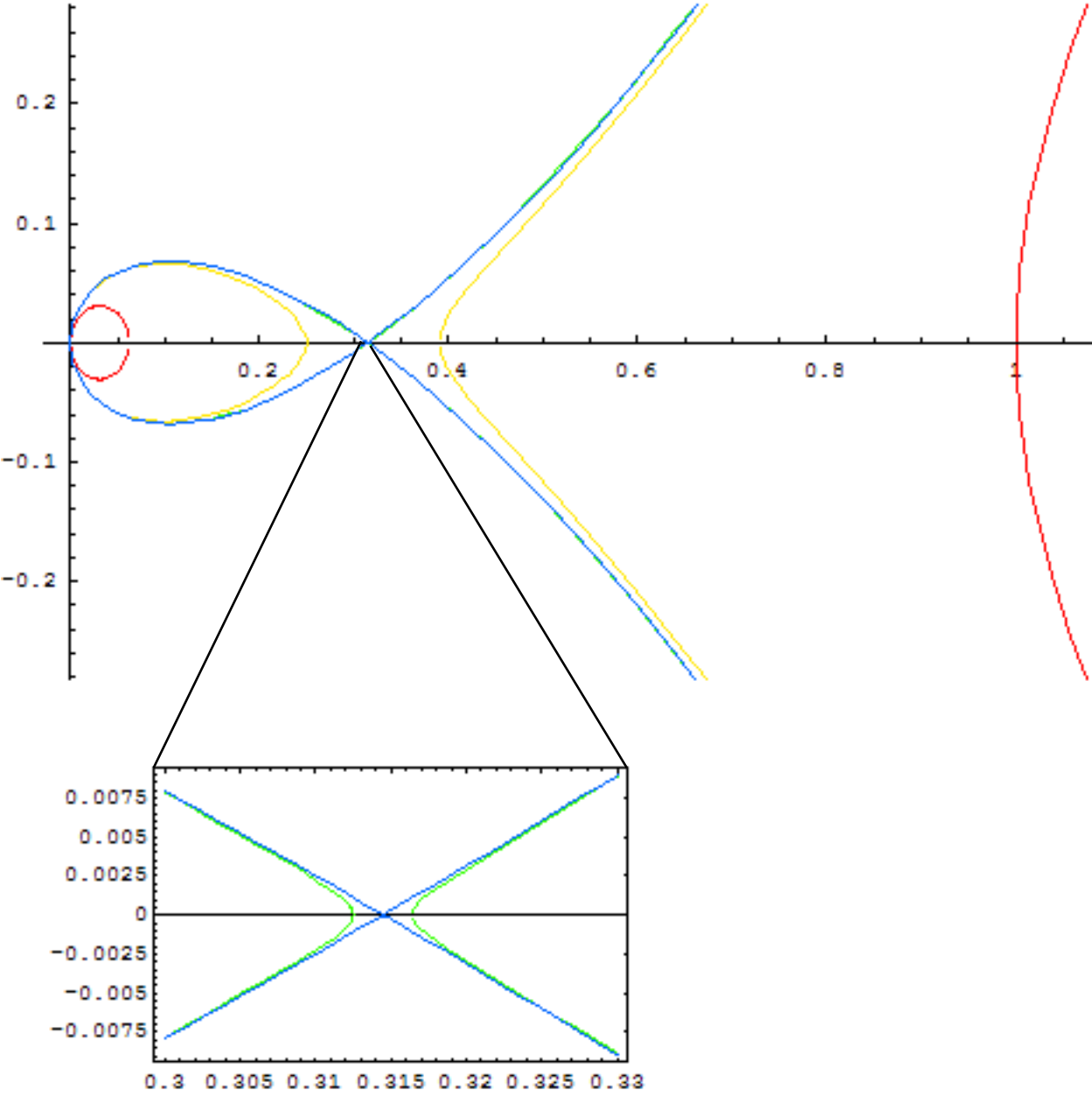
This is useful because the AGM converges very quickly, in fact quadratically, allowing values for elliptic integrals to be calculated. In particular

$$\int_0^1 \frac{dx}{1-x^4} = \frac{\pi}{2M(1, \sqrt{2})}$$

gives a method for efficiently calculating digits of  $\pi$ .

# Example: The AGM for an Elliptic Curve

$$E_0 : y^2 = x(x - 1)(x - \frac{1}{16})$$



- $E_0$
- $E_1$
- $E_2$
- $E_\infty$

## Application: Elliptic Curve Cryptography

The idea of public key cryptography is to create a mathematical puzzle (called *the public key*) which is hard to solve without specific knowledge of how the puzzle was created (*the private key*), and easy to solve with it.

*Ex.* RSA is an example of a public key cryptosystem based on the difficulty of factoring products of large primes.

Another type of puzzle involves solving  $a^b = c$  or  $b$  knowing  $a$  and  $c$ . This is easy for real and complex numbers ( $b = \log c / \log a$ ), but hard for large finite groups, such as the points on an elliptic curve  $E$  over a finite field. This type of puzzle is called a *discrete logarithm system*.

Let  $\mathbb{F}_{2^d}$  be our finite field. The elliptic curve AGM gives us an algorithm to check the number of points on  $E$ , so that we know the puzzle will be hard enough.

## Elliptic Curve Cryptography, cont'd.

**Algorithm** see [8 17.3]

*Input:* elliptic curve  $E : y^2 + xy = x^3 + \bar{c}$  over  $\mathbb{F}_{2^d}$  with  $j(E) \neq 0$

*Output:* number of points on  $E$  in  $\mathbb{F}_{2^d}$

1.  $N := \lceil \frac{d}{2} \rceil + 3$

2.  $a := 1$

$b := 1 + 8c \pmod{2^4}, (c \equiv \bar{c} \pmod{2})$

3. For  $i = 5$  to  $N$  Do  $(a, b) := ((a + b)/2, \sqrt{ab}) \pmod{2^i}$

4.  $a_0 := a$

5.  $t := \frac{a_0}{a} \pmod{2^{N-1}}$

6. If  $t^2 > 2^{d+2}$  Then  $t := t - 2^{N-1}$

7. Print  $2^d + 1 - t$

## References

- [1] Ahlfors, Lars, *Complex Analysis. An introduction to the theory of analytic functions of one complex variable*. 3rd edition, McGraw-Hill Book Co., 1978.
- [2] Borwein, Jonathon A., and Peter B. Borwein. *Pi and the AGM. A Study in Analytic Number Theory and Computational Complexity*. John Wiley & Sons, Inc., New York, 1987.
- [3] Bost, Jean-Benoît, and Jean-François Mestre, *Moyenne arithmético-géométrique et périodes des courbes de genre 1 et 2*, *Gaz. Math.* **38** (1988), 36-64.
- [4] Cox, David, *The arithmetic-geometric mean of Gauss*. *Enseign. Math.* (2) **32** (1985), 275-330.
- [5] Diamond, Fred, and Jerry Shurman. *A First Course in Modular Forms*. Springer Science+Business Media, New York, 2005.

- [6] Egan, Greg. “[www.gregegan.net/SCIENCE/KleinQuartic/KleinQuartic.html](http://www.gregegan.net/SCIENCE/KleinQuartic/KleinQuartic.html)”
- [7] **Handbook of elliptic and hyperelliptic curve cryptography**. Edited by Henri Cohen, et. al. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2006.
- [8] RSA Laboratories. “[www.rsasecurity.com/rsalabs/faq/images/eca.gif](http://www.rsasecurity.com/rsalabs/faq/images/eca.gif)”
- [9] Sethna, Jim. “[www.lassp.cornell.edu/sethna/sethna.html.gif](http://www.lassp.cornell.edu/sethna/sethna.html.gif)”