POLYNOMIALS WITH SMALL ELLIPTIC MAHLER MEASURE VIA GENETIC ALGORITHMS

By

JOHN MICHAEL CLARK

Bachelor of Science in Mathematics
California Institute of Technology
Pasadena, California
2016

Submitted to the Faculty of the
Graduate College of the
Oklahoma State University
in partial fulfillment of
the requirements for
the Degree of
MASTER OF SCIENCE
May, 2020

POLYNOMIALS WITH SMALL ELLIPTIC MAHLER MEASURE

VIA GENETIC ALGORITHMS

Thesis Approved:

Dr. Paul Fili

Thesis Advisor

Dr. Igor Pritsker

Dr. David Wright

ACKNOWLEDGMENTS

I would like to thank Dr. Fili for being such a wonderful advisor. This work was also made possible with the help of the OSU High Performance Computing Center at Oklahoma State University (OSU) supported in part through the National Science Foundation grant OAC-1531128. Special thanks goes to Jesse Schafer, Manager of Operations for the OSU High Performance Computing Center, for help with software setup and installation. I also have to thank my parents for the love and care they have given me and instilled in me from a young age. Finally I would like to praise God for being a stable refuge in good times and bad times. His love enables me to live life to its fullest.

Name: JOHN MICHAEL CLARK

Date of Degree: MAY 2020

Title of Study: SMALL ELLIPTIC MAHLER MEASURE VIA GENETIC ALGORITHMS

Major Field: MATHEMATICS

Abstract: For a minimal polynomial f we denote by $M(f)$ the Mahler measure of the roots of f. The classical Lehmer conjecture is concerned with finding a definitive lower bound for $M(f)$. Lehmer's polynomial is known to have the lowest Mahler measure for all polynomials. We look at a version of Lehmer's conjecture involving elliptic curves and investigate the corresponding Mahler measures, looking for those polynomials with minimal Mahler measure on various elliptic curves. We detail the results we have found using genetic algorithms.

TABLE OF CONTENTS

List of Figures

Figure Page

List of Tables

Chapter I

INTRODUCTION

In 1933, D.H. Lehmer [11] was investigating the asymptotics of ratios of certain cyclotomic polynomials, in order to help generate large primes. In doing so, he gave a measure to these polynomials (now known as the Mahler measure) and could generalize it to noncyclotomic, irreducible polynomials. A question then arose: What was the polynomial with the lowest Mahler measure? Or put another way, do there exist polynomials with Mahler measure arbitrarily close to 1? In the course of his investigations, he found one polynomial, now called Lehmer's polynomial, that so far has the lowest Mahler measure ever found for a noncyclotomic, irreducible polynomial. Lehmer's polynomial $x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$ has Mahler measure $1.176280818\ldots$. This number happened to be one of many studied by Salem in [20, 21].

Many mathematicians have tried their hand at proving what is now called *Lehmer's conjecture* from many different angles. The best asymptotic lower bound for Mahler measures was found by Dobrowolski in 1979 [7]. Smyth [24] showed that non-reciprocal units have a minimal Mahler measure θ_0, which happens to be the smallest Pisot-Vijayaraghavan number; it is also given by the positive root of $x^3 - x - 1$. From a computational perspective, many exhaustive searches have been performed [14, 15], and Mossinghoff has a website [13] detailing the polynomials with the lowest Mahler measure per degree. In 2017 Otmani, Maul, Rhin and Sac-Epée's [17] work with genetic algorithms allowed them to find new polynomials of very high degree, not found in [13], with low Mahler measure.

The generalizations of Lehmer's problem and its close relatives are numerous, and mathematicians still work on them to this day. Amoroso and Dvornicich [1] showed lower bounds exist for the Mahler measure when working with abelian extensions of $\mathbb{Q}$, and Baker and Silverman [3] generalized their results to abelian varieties of arbitrary dimension. Dimitrov [6] has recently uploaded a preprint on the arXiv giving a proof of the Schinzel-Zassenhaus conjecture, which some say is one step away from proving the Lehmer conjecture. Much work has also been done on Mahler measure on elliptic curves and its generalizations [3, 4, 5, 8, 9].

The aim of this thesis is to look at the elliptic Lehmer conjecture from a computational perspective. As in [17] we use genetic algorithms, a hallmark of machine learning, to investigate polynomials of low Mahler measure in the context of elliptic curves. Our results point to an interesting finding which relates the primes of bad reduction for elliptic curves to those polynomials with low Mahler measure. The data for our results can be found online, in a manner somewhat analogous to that of [13], at `https://math.okstate.edu/people/jclark/emmeasure.html`.

The layout of this thesis is as follows. In Section 2 we introduce the relevant tools needed to study Mahler measure, namely the Weil height and dynamical height. In Section 3 we describe the necessary information on elliptic curves, paying close attention to Lattès maps and their properties. In Section 4 we give a brief overview on genetic algorithms. In Section 5 we describe the methodology used to carry out our computations. In Section 6 we give the results of our study on elliptic curves with Weierstrass equation $y^2 = x^3 + ax + b$ where $a, b \in \mathbb{Z}$. Special attention will be made to elliptic curves with complex multiplication (CM), and then non-CM elliptic curves. Lastly we note potential future projects related to this study.

Chapter II

HEIGHT FUNCTIONS

II.1 Weil Height

Rational numbers can be given a measure that corresponds to their complexity. In this case we would say a fraction like $\frac{1}{2}$ is less complex than the fraction $\frac{255}{512}$. In particular, given a rational number of the form $\frac{a}{b}$, we measure its complexity using the logarithmic Weil height $h : \mathbb{Q} \to [0, \infty)$ given by:

$$h(a/b) = \log \max\{|a|, |b|\} = \sum_{p \text{ place}} \log \max\{1, |a/b|_p\}$$

where $\gcd(a, b) = 1$, and $|\cdot|_p$ is the p-adic absolute value.

This height can be extended to arbitrary number fields. For a number field $K/\mathbb{Q}$ with M_K representing the places v of K, we have:

$$h(\alpha) = \sum_{v \in M_K} \frac{[K_v : \mathbb{Q}_p]}{[K : \mathbb{Q}]} \log \max\{1, |\alpha|_v\}$$

where $\alpha \in K^\times$.

The height can be easily computed when we know α is a root of a minimal polynomial $f(x) \in \mathbb{Z}[x]$:

Theorem II.1.1 (Mahler's formula) *Let $\alpha \in K^\times$ have minimal polynomial $f(x) = a_n x^n + \ldots + a_0 \in \mathbb{Z}[x]$. If we factor the polynomial over $\mathbb{C}$ as*

$$f(x) = a_n \prod_{i=1}^{n} (x - \alpha_i),$$

then

$$h(\alpha) = \frac{1}{n} \left(\log|a_n| + \sum_{i=1}^{n} \log \max\{1, |\alpha_i|\} \right).$$

The Mahler measure can now be easily computed for an algebraic integer. Given K a field, $\alpha \in K$ with height $h(\alpha)$, the Mahler measure of α is given by $M(\alpha) = e^{n \cdot h(\alpha)}$. With the above theorem we can compute the Mahler measure to be

$$M(\alpha) = |a_n| \prod_{i=1}^{n} \max\{1, |\alpha_i|\} = \pm a_n \prod_{\substack{i=1 \\ |\alpha_i|>1}}^{n} \alpha_i.$$

Where the overall sign of $M(\alpha)$ is made to be positive.

II.2 Properties of Weil height

The Weil height has many useful properties. In particular:

1. *Kronecker's theorem*: For $\alpha \neq 0$, $h(\alpha) = 0$ if and only if $\alpha \in \mathrm{Tor}(\overline{\mathbb{Q}}^{\times})$, i.e., when α is a root of unity.

2. $h(\alpha^r) = |r| h(\alpha)$ for $r \in \mathbb{Q}$, any choice of root.

3. $h(\alpha\beta^{-1}) \leq h(\alpha) + h(\beta)$.

4. $h(\alpha\zeta) = h(\alpha)$ for all $\zeta \in \mathrm{Tor}(\overline{\mathbb{Q}}^{\times})$.

5. $h(\sigma\alpha) = h(\alpha)$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

The height also gives us information about the size of certain sets:

Theorem II.2.1 (Northcott) *For any number field $K/\mathbb{Q}$ and arbitrary $T \geq 0$,*

$$A_K(T) = \{\alpha \in K : h(\alpha) \leq T\}$$

is a finite set. In fact, for $T, D \geq 0$ fixed,

$$\#\{\alpha \in \overline{\mathbb{Q}} : [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq D \text{ and } h(\alpha) \leq T\} < \infty.$$

II.3 Lehmer Conjecture

We have the following conjecture concerning heights:

Conjecture II.3.1 (Lehmer, 1933) *There exists an absolute constant $c > 0$ such that if $h(\alpha) \neq 0$, then*

$$h(\alpha) \geq \frac{c}{[\mathbb{Q}(\alpha) : \mathbb{Q}]}$$

One should note that Lehmer did not make this conjecture; he merely asked if the Mahler measure can be arbitrarily close to 1. In [11] Lehmer found the polynomial, $x^{10}+x^9-x^7-x^6-x^5-x^4-x^3+x+1$, with the lowest Mahler measure to date. This degree in the lower bound is sharp. Indeed, for α a root of the polynomialx^n-2, one has $[\mathbb{Q}(2^{1/n}) : \mathbb{Q}] \cdot h(2^{1/n}) \geq \log(2)$ for all $n \geq 1$, where $2^{1/n}$ is the real positive root of $x^n - 2$. The following theorem is very close to the desired conjecture:

Theorem II.3.1 (Dobrowolski [7]) *There exists an absolute constant $c > 0$ such that*

$$h(\alpha) \geq \frac{c}{[\mathbb{Q}(\alpha) : \mathbb{Q}]} \cdot \left(\frac{\log\log[\mathbb{Q}(\alpha) : \mathbb{Q}]}{\log[\mathbb{Q}(\alpha) : \mathbb{Q}]}\right)^3$$

for $\alpha \notin \mathrm{Tor}(\overline{\mathbb{Q}}^\times)$.

II.4 Dynamical Heights

The Weil height behaves somewhat nicely with rational functions. If $\varphi(z)$ is a rational function of degree d, then there exist constants depending only on φ such that

$$h(\varphi(\alpha)) = d \cdot h(\alpha) + O(1).$$

We would like to get rid of these big-O constants. To do so, we replace our height function h with a new height function h_φ known as the Call-Silverman height, or dynamical height. It has the property that

$$h_\varphi(\varphi(\alpha)) = d \cdot h_\varphi(\alpha).$$

Specifically, it is given by

$$h_\varphi(\alpha) = \lim_{n\to\infty} \frac{1}{d^n} h(\varphi^n(\alpha))$$

where $\varphi^n = \varphi \circ \ldots \circ \varphi$ denotes n-fold iteration. Given the iterative aspect of the dynamical height, the dynamical properties of φ do in fact play a role. If we define the *preperiodic points* of φ by

$$\mathrm{PrePer}(\varphi) = \{\alpha \in \mathbb{P}^1(\overline{\mathbb{Q}}) : \varphi^n(\alpha) = \varphi^m(\alpha) \text{ for some } m \neq n, \quad m, n \geq 0\}$$

and the *periodic points* by

$$\mathrm{Pre}(\varphi) = \{\alpha \in \mathbb{P}^1(\overline{\mathbb{Q}}) : \varphi^n(\alpha) = \alpha \text{ for some } n \in \mathbb{N}\}$$

then we have:

Lemma II.4.1 *Let φ be a rational function of degree d. Then the dynamical height h_φ satisfies the following properties:*

1. $h_\varphi(\varphi(\alpha)) = d \cdot h_\varphi(\alpha)$.

2. *There exists constants depending only on φ such that*

$$h_\varphi(\alpha) = h(\alpha) + O(1)$$

   for all $\alpha \in \mathbb{P}^1(\overline{\mathbb{Q}})$.

3. *h_φ satisfies the Northcott property, as stated above.*

4. $h_\varphi(\alpha) = 0 \iff \alpha \in \mathrm{PrePer}(\varphi)$.

We also have a way of classifying dynamical heights:

Theorem II.4.1 (Petsche, Szpiro, Tucker [18]) *Given two rational maps φ, ψ of degree at least 2, then the following are equivalent:*

1. $h_\varphi = h_\psi$.

2. $\mathrm{PrePer}(\varphi) = \mathrm{PrePer}(\psi)$.

3. $\mathrm{PrePer}(\varphi) \cap \mathrm{PrePer}(\psi)$ *is infinite.*

4. $\liminf_{\alpha \in \overline{\mathbb{Q}}} h_\varphi(\alpha) + h_\psi(\alpha) = 0$, *i.e., there is a sequence of points which is small for both maps simultaneously.*

There is also a corresponding conjecture for dynamical height:

Conjecture II.4.1 (Dynamical Lehmer) *Let φ be a rational map of degree at least 2 defined over a number field K. Then there exists an absolute constant $c > 0$ depending only on φ and K such that for all $\alpha \in \overline{K}$ that are not preperiodic for φ,*

$$h_\varphi(\alpha) \geq \frac{c}{[K(\alpha) : K]}.$$

Chapter III

ELLIPTIC CURVES

Here we introduce the necessary material concerning elliptic curves. Our presentation largely follows [23]. An elliptic curve $E(K)$ is defined over a field K. We omit K and refer to an elliptic curve only as E when the context is clear. We also omit proofs for brevity.

III.1 Definition and Group Law

An elliptic curve $E(\mathbb{Q})$ can be described as the set of solutions (x, y) to a Weierstrass equation of the form

$$y^2 = x^3 + ax + b,\ \ a, b \in \mathbb{Q}$$

along with an extra "point at infinity" $\mathcal{O}$. We will often refer to the elliptic curve with Weierstrass equation $y^2 = x^3 + ax + b$ by $E_{a,b}$. To ensure that the curve is smooth - i.e. has no cusps or self-intersections - we require that $4a^3 + 27b^2 \neq 0$. The discriminant $\Delta(E_{a,b})$ and j-invariant $j(E_{a,b})$ are defined by the formulas

$$\Delta(E_{a,b}) = -16(4a^3 + 27b^2)$$
$$j(E_{a,b}) = 1728\frac{4a^3}{4a^3 + 27b^2}$$

For a general field K we require that its characteristic not be 2 or 3, otherwise we must use a more general equation for the elliptic curve.

The j-invariant gives us a way of classifying elliptic curves: two elliptic curves E and E' defined over a field K are isomorphic over $\overline{K}$ if and only if $j(E) = j(E')$.

Elliptic curves can be embedded in the projective plane $\mathbb{P}^2(\mathbb{Q})$. They are then defined by the homogeneous equation

$$Y^2Z = X^3 + aXZ^2 + bZ^3,$$

where the point at infinity can now be explicitly given as $[0, 1, 0]$.

An elliptic curve can be made into a group with an operation that is somewhat intuitive when considered geometrically. Given two points P, Q on the elliptic curve E, a line through them will intersect E at a third point R. The group law for E stipulates that $P + Q + R = \mathcal{O}$. Here $\mathcal{O}$ plays the role of the identity, so that $P + Q = -R$. The inverse of the point $P = [X, Y, Z]$ is given by $-P = [X, -Y, Z]$. To show the operation is associative is rather tedious, so we shall not demonstrate it here.

III.2 Lattès maps

We are interested in the morphisms that act on elliptic curves. We do so by looking at Lattès maps. We start with some preliminaries.

Let E_1 and E_2 be two elliptic curves. An *isogeny* between E_1 and E_2 is a surjective morphism $\psi : E_1 \to E_2$ such that $\psi(\mathcal{O}) = \mathcal{O}$. One can show that an isogeny is a homomorphism of groups. Then

$$\psi(P + Q) = \psi(P) + \psi(Q) \quad \text{for all } P, Q \in E_1\bar{(}K).$$

For an elliptic curve E, the *endomorphism ring of* E, which we denote $\mathrm{End}(E)$, is the set of isogenies from E to itself, with addition and multiplication given by

$$(\psi_1 + \psi_2)(P) = \psi_1(P) + \psi_2(P), \quad (\psi_1\psi_2)(P) = \psi_1(\psi_2(P)).$$

The *automorphism group of* E, $\mathrm{Aut}(E)$, is the set of bijective endomorphisms. Put another way, $\mathrm{Aut}(E) = \mathrm{End}(E)^{\times}$ is the group of units in $\mathrm{End}(E)$.

Every integer m has a corresponding *multiplication-by-*m morphism in $\mathrm{End}(E)$. For $m > 0$ this is naturally given by

$$[m] : E \to E, \quad [m]\,(P) = \overbrace{P + P + \ldots + P}^{m \text{ terms}}.$$

If $m < 0$ then $[m]\,(P) = -\,[-m]\,(P)$. When $m = 0$ we have $[m]\,(P) = O$. This embeds $\mathbb{Z}$ into $\mathrm{End}(E)$. In characteristic 0 most elliptic curves have no other endomorphisms.

When an elliptic curve E *does* have more endomorphisms, we say that E has *complex multiplication* or "CM".

For example, the elliptic curves $E_{a,0}$ and $E_{0,b}$ have CM. Letting μ_n refer to the group of n^{th} roots of unity and $\rho = (-1 + \sqrt{-3})/2$ denote a cube root of unity, we have

$$E_{a,0} : y^2 = x^3 + ax, \quad j(E_{a,0}) = 1728, \quad \mathrm{End}(E_{a,0}) = \mathbb{Z}\,[i]\,, \quad \mathrm{Aut}(E_{a,0}) = \mu_4,$$
$$E_{0,b} : y^2 = x^3 + b, \quad j(E_{0,b}) = 0, \quad \mathrm{End}(E_{0,b}) = \mathbb{Z}\,[\rho]\,, \quad \mathrm{Aut}(E_{0,b}) = \mu_6.$$

Here $[i]$ and $[\rho]$ can be thought of as the maps

$$[i]\,(x, y) = (-x, iy), \quad [\rho]\,(x, y) = (\rho x, y).$$

One can verify that $[i]^2\,(P) = -P$ and $[\rho]^3\,(P) = P$. So $[i]^2$ is the same as the map $[-1]$, and $[\rho]^3$ is the same as the identity map.

Note that though the elliptic curves are isomorphic over $\overline{\mathbb{Q}}$, they might not be isomorphic over $\mathbb{Q}$.

The automorphisms of an elliptic curve can be described as follows:

Theorem III.2.1 *Let K be a field whose characteristic is not equal to 2 or 3 and let*

E/K be an elliptic curve. Then

$$\mathrm{Aut}(E) = \begin{cases} \mu_2, & \text{if } j(E) \neq 0 \text{ and } j(E) \neq 1728, \\ \mu_4, & \text{if } j(E) = 1728, \\ \mu_6, & \text{if } j(E) = 0. \end{cases}$$

If we quotient E by a finite group of automorphisms, then we get a map from E to $\mathbb{P}^1$.

Theorem III.2.2 *Let Γ be a nontrivial subgroup of $\mathrm{Aut}(E)$. Then the quotient curve E/Γ is isomorphic to $\mathbb{P}^1$ and a projection map $\pi : E \to E/\Gamma \cong \mathbb{P}^1$ can be given explicitly by*

$$\pi(x, y) = \begin{cases} x, & \text{if } \quad \Gamma = \mu_2 \quad (j(E) \text{ arbitrary}), \\ x^2, & \text{if } \quad \Gamma = \mu_4 \quad (j(E) = 1728 \text{ only}), \\ y, & \text{if } \quad \Gamma = \mu_3 \quad (j(E) = 0 \text{ only}), \\ x^3, & \text{if } \quad \Gamma = \mu_6 \quad (j(E) = 0 \text{ only}). \end{cases}$$

With all the necessary pieces, we now work with Lattès maps. Given an elliptic curve E, a morphism $\psi : E \to E$, and a finite separable covering $\pi : E \to \mathbb{P}^1$, a *Lattès map* is a rational map $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ of degree $d \geq 2$ that can be defined in such a way that the following diagram commutes:

$$\begin{array}{ccc} E & \xrightarrow{\psi} & E \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi} \\ \mathbb{P}^1 & \xrightarrow{\phi} & \mathbb{P}^1 \end{array}$$

For example, if we let $\psi = [2]$ be the doubling map, $\pi(x, y) = x$, then ϕ can be found by the relation $\phi \circ \pi(P) = \pi \circ [2]\,(P)$. In other words, *one can compute the output of the Lattès map on an x-coordinate of a point P, by finding the x-coordinate of $2P$.* In particular, for the elliptic curve $E_{a,b}$,

$$\phi(x) = \frac{x^4 - 2ax^2 - 8bx + a^2}{4x^3 + 4ax + 4b}.$$

If we use the curve $E_{a,0}$, this map becomes

$$\phi(x) = \frac{(x^2-a)^2}{4x(x^2+a)}.$$

However we also have access to the projection $\pi(x,y) = x^2$, and thus get the new Lattès map

$$\phi'(x) = \frac{(x-a)^4}{16x(x+a)^2}.$$

Using the curve $E_{0,b}$, our standard Lattès map becomes

$$\phi(x) = \frac{x(x^3-8b)}{4(x^3+b)}$$

and the two projections $\pi_1(x,y) = y, \quad \pi_2(x,y) = x^3$ give us two other Lattès maps, respectively

$$\phi_1(y) = \frac{y^4+18by^2-27b^2}{8y^3}, \quad \phi_2(x) = \frac{x(x-8b)^3}{64(x+b)^3}.$$

Notice that these are all degree 4 maps. With these maps we have dynamical heights h_ϕ corresponding to each one, where $h_\phi(\phi(\pi(P))) = 4h_\phi(\pi(P))$, where $P \in E(\mathbb{Q})$. For convenience let $\hat{h}(P) = h_\phi(\pi(P))$. This is also known as the Néron-Tate height for the elliptic height E, and actually provided inspiration for the more general Call-Silverman dynamical height. We now state the analogue of the Dynamical Lehmer conjecture for elliptic curves:

Conjecture III.2.1 (Elliptic Lehmer Conjecture) *Let ϕ be a rational function over the elliptic curve E over the field K. Then there exists an absolute constant $c > 0$ depending only on E and K such that for all P not contained in the torsion subgroup of E,*

$$\hat{h}(P) \geq \frac{c}{[K(P):K]}.$$

For us $[\mathbb{Q}(P):\mathbb{Q}(x)] \leq 2$. We really only care for x because y is determined by x up to a factor of -1. The quadratic nature of the y-coordinate also makes $[\mathbb{Q}(P):\mathbb{Q}]$ at most double that of $[\mathbb{Q}(x):\mathbb{Q}]$.

Lower bound for $\hat{h}(P)$	**Restrictions**	**Reference**
$cD^{-\kappa}$	none	Masser (1984) [12]
$cD^{-\frac{1}{g}}\left(\frac{\log\log(3D)}{\log(3D)}\right)^{\kappa}$	CM, $g = g_0(P)$	David-Hindry (2000) [5]
c	$P \in A(K^{ab})$ K totally real	Zhang (1998) [26]
c	$P \in A(K^{ab})$ $g = 1$	Baker, Silverman (2003) [2, 22]

Table III.1: History of lower bounds for $\hat{h}$ in $A(\overline{K})$.

Letting $D(P) = [K(P) : K]$, it is known that for a Lattès map ϕ defined over a number field K:

$$\hat{h}_{\phi}(P) \geq \begin{cases} \dfrac{c}{D(P)^3 \log^2 D(P)} & \text{in general[12],} \\ \dfrac{c}{D(P)^2} & \text{if } j(E) \text{ is nonintegral[10],} \\ \dfrac{c}{D(P)}\left(\dfrac{\log\log D(P)}{\log D(P)}\right)^3 & \text{if } E \text{ has CM[5].} \end{cases}$$

Let A/K be an abelian variety of dimension g defined over a number field K, and let K^{ab} be the maximal abelian extension of K. Let $\mathcal{L}$ be a symmetric ample line bundle on A/K, and let $\hat{h} : A(\overline{K}) \to \mathbb{R}$ be the associated canonical height function. Let also $P \in A(\overline{K})$ be a nontorsion point, and $D = [K(P) : K]$. Then there exists a positive constant c depending on A/K and on $\mathcal{L}$, but not on P, and a positive constant κ depending only on g such that the lower bounds in Table III.1 hold.

As a side note, a map similar to the Lattès map is given by the *Chebyshev polynomials* T_d for $d > 1$, which are defined so that the following diagram commutes:

$$\begin{array}{ccc} \overline{\mathbb{Q}}^\times & \xrightarrow{z \mapsto z^d} & \overline{\mathbb{Q}}^\times \\ {\scriptstyle z \mapsto z + z^{-1}} \downarrow & & \downarrow {\scriptstyle z \mapsto z + z^{-1}} \\ \overline{\mathbb{Q}} & \xrightarrow{T_d} & \overline{\mathbb{Q}} \end{array}$$

For example, $T_2(z) = z^2 - 2$. In all cases $T_d(z) \in \mathbb{Z}[z]$, and the unit circle is sent to the set $E = [-2, 2]$. As shown by Rumely in [19], one can define a new height function for E, and get a corresponding Lehmer conjecture there. Moreover, the Lehmer conjecture for E and the classical Lehmer conjecture are actually equivalent!

III.3 Reduction Modulo p

Let K be a local field with ring of integers R, maximal ideal $\mathfrak{p}$, and residue field $k = R/\mathfrak{p}$. Let $\tilde{x}$ be the reduction of x modulo $\mathfrak{p}$.

If E is an elliptic curve defined over K, then a *minimal Weierstrass equation for* E is a Weierstrass equation whose discriminant $\Delta(E)$ has minimal valuation, where all the coefficients of the Weierstrass equation are in R.

As an example, if k does not have characteristic 2 or 3, then a Weierstrass equation for the elliptic curve $E_{a,b}$ is minimal if and only if

$$a, b \in R \quad \text{and} \quad \min\{3 \operatorname{ord}_{\mathfrak{p}}(a), 2 \operatorname{ord}_{\mathfrak{p}}(b)\} < 12.$$

Luckily there is an algorithm due to Tate that can convert a Weierstrass equation into a minimal Weierstrass equation.

Once we have a minimal Weierstrass equation for E/K, we can reduce the coefficients of E to get a curve $\tilde{E}/k$. We say that E has *good reduction* if $\tilde{E}$ is nonsingular. This occurs if and only if $\Delta(E)$ is a unit in R. An elliptic curve has *bad reduction* if it does not have good reduction. In either case, we get a *reduction modulo* $\mathfrak{p}$ *map* on points,

$$E(K) \to \tilde{E}(k), \quad P \mapsto \tilde{P}.$$

One can show that if E has good reduction, then the reduction modulo $\mathfrak{p}$ map $E(K) \to \tilde{E}(k)$ is a homomorphism.

Suppose our elliptic curve E is defined over a number field K, and let $\mathfrak{p}$ be a prime of K. If the coefficients of E's Weierstrass equation are $\mathfrak{p}$-adic integers, and $\Delta(E)$ is a $\mathfrak{p}$-adic unit, then we say has good reduction at $\mathfrak{p}$.

As an example, the elliptic curve $E_{0,1} : y^2 = x^3 + 1$ has discriminant $\Delta(E_{0,1}) = -16 \cdot 27$, and therefore has good reduction at prime 5. However it has bad reduction at primes 2 and 3.

The primes where our elliptic curve has bad reduction are interesting to our study, as our data will reveal.

III.4 Torsion points

The kernel of an endomorphism can be an important tool when determining the arithmetic properties of its associated elliptic curve.

Let E be an elliptic curve. Given an endomorphism $\psi \in \mathrm{End}(E)$, let

$$E[\psi] = \mathrm{Ker}(\psi) = \{P \in E(\overline{K}) : \psi(P) = \mathcal{O}\}.$$

We pay special attention to the kernel of the multiplication-by-m map,

$$E[m] = \{P \in E(\overline{K}) : [m](P) = \mathcal{O}\}.$$

$E[m]$ is known as the *m-torsion subgroup of E*. The *torsion subgroup of E* is the union of all the $E[m]$:

$$E_{\mathrm{tors}} = \bigcup_{m \geq 1} E[m].$$

Theorem III.4.1 *Let K be a local field whose residue field has characteristic p, let E/K be an elliptic curve with good reduction, and let $m \geq 1$ be an integer with $p \nmid m$. Let $E(K)[m] = E[m] \cap E(K)$, so $E(K)[m]$ is the subgroup of $E[m]$ containing points with coordinates in K. Then the reduction map*

$$E(K)[m] \to \tilde{E}(k)$$

is one-to-one, so different m-torsion points map to different reductions modulo $\mathfrak{p}$.

Our study of Lattès maps leads us to the following useful characterization of the periodic points of a Lattès map.

Theorem III.4.2 *Let ϕ be a Lattès map associated to an elliptic curve E. Then*

$$\text{PrePer}(\phi) = \pi(E_{\text{tors}}).$$

This provides an analogue to Kronecker's theorem and part 4 of lemma II.4.1. The preperiodic points of the Lattès map are exactly those which are the x-coordinates of points lying in the torsion subgroup of E. Another way of saying this is that the preperiodic points of our Lattès map ϕ are projections of the preperiodic points of the doubling map [2].

We get a similar result for the Chebyshev maps as well. If we let $\pi(z) = z + z^{-1}$ be our projection, then the preperiodic points of the dth Chebyshev polynomial are the projections of the preperiodic points of the d-power map; these are the roots of unity! For example, the preperiodic points of T_2 are $\zeta_n + \zeta_n^{-1}$ for $n = 2^k$.

Chapter IV

GENETIC ALGORITHMS

In an effort to study the classical Lehmer conjecture, many mathematicians have tried increasingly sophisticated ways of finding polynomials with low Mahler measure. The search can be reframed in terms of a optimization, and genetic algorithms provide a natural way of doing so. Following the terminology of [17], each polynomial can be thought of as a point in the optimization phase space. By expressing a polynomial $\sum_{n=0}^{d} a_n x^n$ in terms of its coefficients $(a_d, \ldots, a_0)$, we seek the point that minimizes the function

$$M^*(a_d, \ldots, a_0) = M(\alpha)$$

where α is a root of the minimal polynomial $\sum_{n=0}^{d} a_n x^n$. We restrict $a_d \neq 0$ so that our polynomials are of the proper degree. It is easy to see that $M(\alpha) \geq 1$, and that for polynomials f and g, $M(fg) = M(f) \cdot M(g)$. Thus we only have to check over minimal polynomials with Mahler measure not equal to 1. To minimize M^*, we use the following algorithm, which is also given in Figure IV.1 below:

Generate population We randomly generate polynomials for a given degree d, by choosing the coefficients from a set D randomly. This is the first generation.

Score and sort Next we score each polynomial according to its Mahler measure and sort them by magnitude.

Selection The n polynomials with the lowest Mahler measures are designated as special candidates for crossbreeding.

Crossbreeding The remaining polynomials are replaced with crossbred versions of the n best polynomials. Two parent polynomials are chosen, and their genes are mixed to produce a new child polynomial with (hopefully) lower Mahler measure.

Mutation All of the polynomials, except for a certain number with the lowest Mahler measures, are then given the chance to mutate. That is, each polynomial has a small chance of its genes being altered in some small, controllable way.

Repeat The polynomials are then re-scored and resorted. After a given number of repetitions, called generations, the polynomial with the lowest Mahler measure is reported.

As can be expected, these genetic algorithms can be rather slow, especially when having to ensure that the polynomials obey our constraints that they are irreducible, and not have Mahler measure 1. However, they do provide a reliable way, given enough time, of providing polynomials with low Mahler measure. The authors of [17] were able to find new polynomials of high degree with surprisingly low Mahler measure using this technique. We would like to extend this technique to the realm of polynomials defined over elliptic curves.

To associate each polynomial $p(x)$ to the elliptic curve $E : y^2 = x^3 + ax + b$, we first compute a root of the polynomial, denoted x_0. We then solve the equation $y^2 = x_0^3 + ax_0 + b$ for y. Here the choice of root does not matter, since $\hat{h}(-P) = \hat{h}(P)$. If we denote this square root as y_0, then we let the point (x_0, y_0) represent our polynomial on the elliptic curve. Then we compute the height of this point on the elliptic curve, and let that be the height of the associated polynomial on the curve.

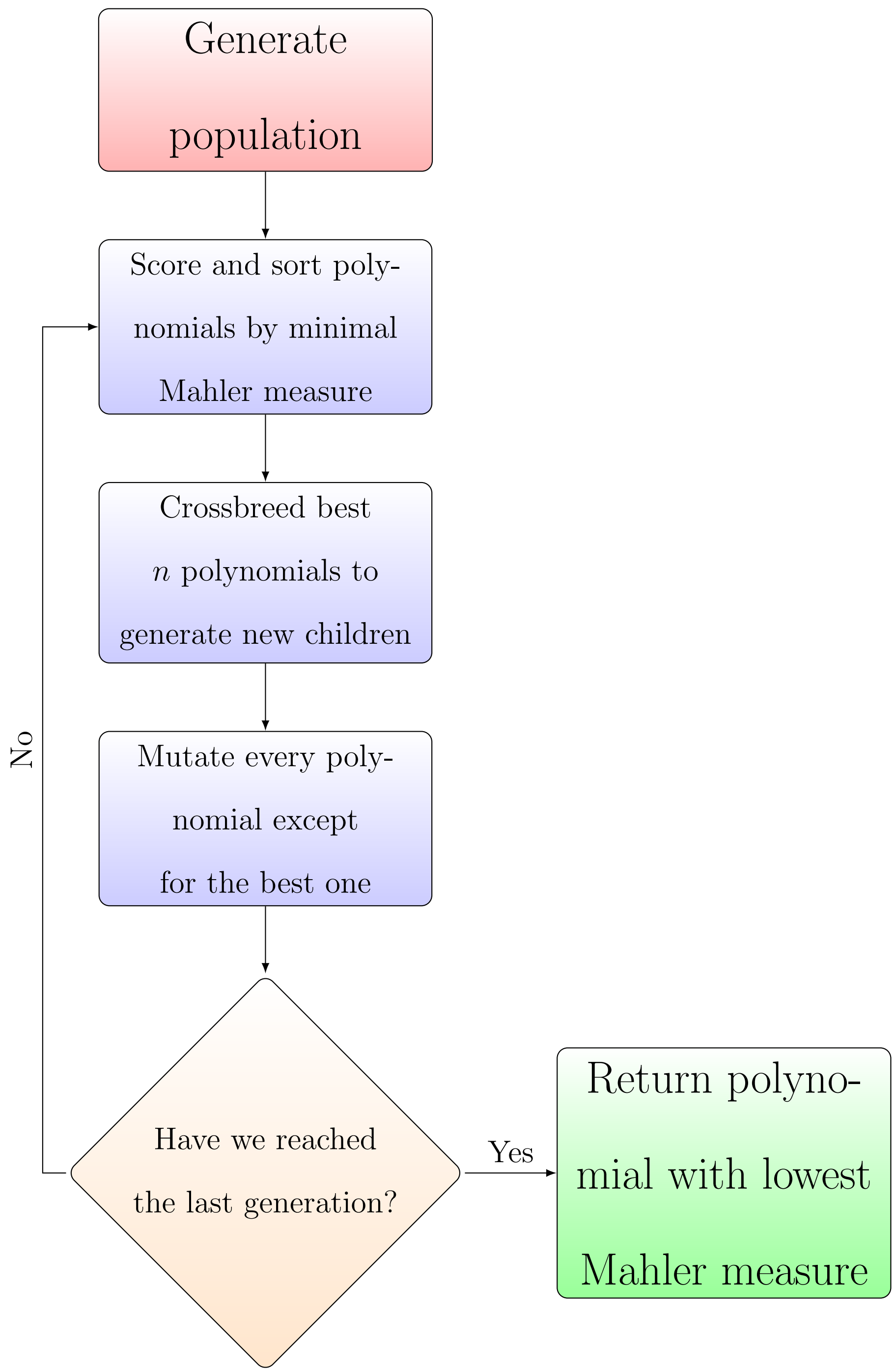

Figure IV.1: Genetic Algorithm diagram

Chapter V

METHODOLOGY

We ran our genetic algorithm on elliptic curves with Weierstrass equation $y^2 = x^3 + ax + b$ using the following parameters:

Linear term This determined the a coefficient for our elliptic curves, and ranged over the integers.

Constant term This determined the b coefficient for our elliptic curves, and ranged over the integers. Since the equation $y^2 = x^3$ has discriminant 0, the singular elliptic curve represented by $E_{0,0}$ was not used in our computation. However the remaining 99 elliptic curves did have nonzero discriminant, and were therefore included in the analysis.

Degree To ease computation, for a given elliptic curve the genetic algorithm would only work on polynomials of a given degree per run. This was also helpful because Mahler measure generally goes up with degree, so the degree restraint prevented polynomials with low degree from completely filling our population, and thereby hiding information on polynomials with high degree with potentially low Mahler measure. For our study we used degrees 1 through 10.

Population Size For each run we used a population of 200 polynomials, whose size did not change. Given the natural filtering in our algorithm, this often led to certain polynomials with small Mahler measure showing up repeatedly in the population. This will be expounded when we describe the mutation process.

Generations While we could have let the search go on for quite a long time (in fact, never having it stop if we wanted to), the algorithm generally converged on a given polynomial with lowest Mahler measure within 50 generations. To allow for potential improvements, we set the algorithm to stop after 100 generations.

Best population size To increase genetic diversity, after each generation we preserved the 50 polynomials in our population with the lowest Mahler measures and crossbred them. These new polynomials then replaced the remaining 150 polynomials in the population.

Mutation rate To increase genetic diversity, after crossbreeding each polynomial (except for the polynomial with the lowest Mahler measure) would be given a chance to mutate, based on a given mutation rate. To keep the population relatively stable, and thereby preserve some of the computational effort already expended, this mutation rate was initially rather low, at a starting value of 10%.

We initially set each run with polynomials having coefficients randomly chosen from the integers $\{-10, \ldots, 10\}$. These integers were chosen according to a uniform distribution.These integers were chosen since the Mahler measure generally increases as the absolute value of the coefficients of our polynomials increase.

However we also found that using a Gaussian distribution greatly speeds up the computation for our study. We did two genetic searches on the elliptic curve $E_{0,1}$. One used a uniform distribution on the integers $\{-50, \ldots, 50\}$, and the other used a Gaussian distribution with mean 0 and standard deviation 20. To ensure the coefficients from our sample were integers, we used a discrete random sampler in Sage. With that implementation, integers $\{-120, \ldots, 120\}$ could show up as potential coefficients. The results of these searches will be given in the next section.

V.1 Increasing Genetic Diversity

As mentioned above, genetic algorithms need some way to increase the space of solutions they check. Otherwise after sorting one time the algorithm would be finished. This space enlargement is generally known as *increasing the genetic diversity*, since our subjects in our population will have their *genes* altered. Polynomials have a natural candidate for genes: their coefficients. In our study the genetic diversity was increased in two ways: crossbreeding and mutation.

To crossbreed the polynomials, two polynomials were chosen at random from the 50 polynomials in the population with the lowest Mahler measure. To ease explanation, consider two polynomials with same degree d: $\sum_{n=0}^{d} a_n x^n$, $\sum_{n=0}^{d} b_n x^n$. A new crossbred version of the two polynomials is given by $\sum_{n=0}^{d} c_n x^n$, where c_n is chosen randomly from $\{a_n, b_n\}$ for $n \in \{0, \ldots, d\}$. After checking that the polynomial is irreducible and the point it represents on the elliptic curve is nontorsion, the polynomial is then added to the population.

Crossbreeding has a limitation, however. After many generations, the population will end up with many copies of a small number of polynomials with low Mahler measure. At worst, one may have a population containing copies all of one polynomial. To combat this, members of the population are given a chance to mutate.

Mutation must be controlled to avoid ruining the population. The members should not change too much from their initial state. Therefore the mutation rate should generally be low to begin with. Should mutation occur, we enact it by taking a polynomial and swap two of its coefficients, chosen at random.

However, sometimes this may not be enough to produce enough genetic diversity in the population. We accomplish this by making the mutation rate *variable*. Let n represent the population size, let k represent the number of *unique* polynomials in the population. Then given a mutation rate μ_0, our new mutation rate would be given by

$$\mu = \mu_0 - 0.1 + \left(\frac{n-k}{n}\right)^{\alpha}$$

where for our study we let $\alpha = 2$. This mutation rate would be allowed to update in this manner once every 10 generations. Observe, the mutation rate generally goes down based on how many generations are left in the algorithm, but also goes up according to the number of unique polynomials in the population. If the mutation rate μ goes above 100%, then let $\mu_n = \lfloor \mu \rfloor$, $\mu_r = \mu - \mu_n$. Then a polynomial would be guaranteed to randomly swap its coordinates μ_n times, and given a chance to swap its coordinates again based on μ_r.

Chapter VI

RESULTS

The following results are based on the computations we ran in this study. We use the logarithmic Mahler measure (which we refer to in tables as Mahler measure*), so values may be less than 1, but greater than 0. For reference, in the classical case Lehmer's polynomial has a logarithmic Mahler measure of 0.162357612.... When we refer to elliptic curves, the notation (a, b) in the tables will refer to the elliptic curve $E_{a,b}$ with Weierstrass equation $y^2 = x^3 + ax + b$.

The following tables (VI.1,VI.2) give the polynomials with the lowest logarithmic Mahler measure for each elliptic curve. Notice that none of the polynomials are reciprocal, i.e. their coefficients do not read the same backwards and forwards. This is very unlike the classical case for Lehmer's conjecture. Another departure we've found is that nonmonic polynomials in our study showed up as having the Mahler measure. This never happens for the classical Lehmer conjecture. Also for each curve the lowest Mahler measure was usually found in polynomials with degree less than or equal to 3. This is to be expected, as the Mahler measure generally increases with degree.

As in the classical Lehmer conjecture, polynomials can have the same Mahler measure when the polynomials are intrinsically related. For example, given the polynomial $f(x)$, polynomials $-f(x), f(-x)$ and $-f(-x)$ will have the same Mahler measure as $f(x)$. This also holds when replacing x with some other root of unity ζ_n, provided the coefficients are still integral. Tables VI.6, VI.7 provide a good example of this.

However, in our study sometimes polynomials of different degrees would tie for being the polynomial with the lowest Mahler measure. This can occur when the point representing the polynomial on the elliptic curve happens to be in the forward orbit of the other point.

For example, the elliptic curve $E_{2,1}$ has polynomials x and $f(x) = x^4 - 4x^2 - 8x + 4$ which have the same elliptic Mahler measure. If we let P represent the point for f, and Q represent the point for x, it turns out that $Q = 2P$. Let ω be a root for f. Since the Neron-Tate height satisfies $\hat{h}(2P) = 4\hat{h}(P)$, and the degree of the field extension for f is $[\mathbb{Q}(\omega) : \mathbb{Q}] = 4$, we get a cancellation that gives $\hat{h}(P)$. This suggests that one can find polynomials of degree 4^n with low elliptic Mahler measure, so long as they are in the backwards orbit of Q under the doubling map, though much more study needs to be done, and it was out of the scope of the current study investigate polynomials with higher degree.

What is most interesting in our study is that for elliptic curves of the form $E_{a,0}$, the constant term for the polynomials were a prime power, or were divisible by primes for which the elliptic curve had bad reduction. These primes also showed up in the other coefficients for some polynomials for other elliptic curves, which suggests some deeper phenomenon may be at play here.

In the appendix we also have tables (Table 1) for all the non-CM curves in our study, along with tables listing the polynomials with lowest Mahler measure per degree for elliptic curves $E_{5,0}$ and $E_{3,3}$ in Tables 2 and 3 respectively.

VI.1 Distributions

As mentioned in the previous chapter, we also investigated what effect using different distributions would have on computation time. The results of our searches give us the data in tables VI.3 and VI.4 below. We can see that the Gaussian search took about one day to finish its search, whereas the uniform search took two days to finish. We can also see that for the first five degrees, the results between the two were very similar, with the Gaussian search actually beating the uniform search for degrees three and five. For degrees six through ten, the results were mixed. The uniform search actually beat the Gaussian search for degrees six, nine and ten, which suggests the uniform search may be more robust for higher degrees. This also makes sense given the way the Gaussian search chooses polynomial coefficients; they are usually close to zero. The coefficients of the lowest degree polynomials in the uniform search were generally farther away from zero. Certain polynomials also took longer to compute the logarithmic Mahler measure for, which likely influenced the computation time as well.

Regardless, it is clear from the data that using Gaussian searches is more viable given the time it takes for them to finish. In the time it takes to complete one uniform search, two Gaussian searches are likely to have already completed. This gives more data for us to work with.

VI.2 Negative values of a and b

For our initial data gathering we explicitly chose our linear and constant parameters to be nonnegative. Later we also took the time to investigate some elliptic curves with negative values as well. For these we used a Gaussian search to find our polynomials. The data for $E_{0,-1}$, $E_{-1,0}$ and $E_{-1,-1}$ are given in Tables VI.5, VI.6, VI.7, VI.8 below.

We can see that primes of bad reduction still appear in our polynomials. It is interesting though that $E_{-1,0}$, with its discriminant a large prime power of two, is more random with its coefficients than we would expect. More tests should be run for this curve to see if this is specific to the search or our elliptic curve.

Elliptic Curve	**Discriminant**	**Polynomial(s)**	**Mahler measure***
$(1,0)$	$-1 \cdot 2^6$	x^3+3x^2-x+1 x^3-3x^2-x-1 x^3-x^2+3x+1 x^3+x^2+3x-1	0.849449656184276
$(2,0)$	$-1 \cdot 2^9$	$x^2+4x-2,\ x^2-4x-2$	0.501182392047178
$(3,0)$	$-1 \cdot 2^6 \cdot 3^3$	$x^2-6x+3,\ x^2+2x+3$	0.250591196023589
$(4,0)$	$-1 \cdot 2^{12}$	$x^2+x+2,\ x^2+2x+8$	0.747220376900835
$(5,0)$	$-1 \cdot 2^6 \cdot 5^3$	$3x^2+5$	1.00236478409436
$(6,0)$	$-1 \cdot 2^9 \cdot 3^3$	x^2-4x+6	0.844190799324968
$(7,0)$	$-1 \cdot 2^6 \cdot 7^3$	$3x^2+7$	1.00236478409436
$(8,0)$	$-1 \cdot 2^{15}$	$x^2-8x-8,\ x^2+8x-8$	0.501182392047179
$(9,0)$	$-1 \cdot 2^6 \cdot 3^6$	$x^2+3x+9,\ x^2+2x+9$	0.888625874839619

Table VI.1: Polynomials with lowest logarithmic Mahler measure for elliptic curves with Weierstrass equation $y^2 = x^3 + ax$

Elliptic Curve	**Discriminant**	**Polynomial**	**Mahler measure***
$(0,1)$	$-1 \cdot 2^4 \cdot 3^3$	$x^3 - 2x^2 - 4x - 4$	0.577051381860240
$(0,2)$	$-1 \cdot 2^6 \cdot 3^3$	$x^3 - 3x^2 - 4$	0.251525634393743
$(0,3)$	$-1 \cdot 2^4 \cdot 3^5$	$x^3 - 6$	0.450320685639875
$(0,4)$	$-1 \cdot 2^8 \cdot 3^3$	$x - 2,\ x^2 - 4x - 8$	0.300213790426584
$(0,5)$	$-1 \cdot 2^4 \cdot 3^3 \cdot 5^2$	$x + 2,\ x^2 - 2x + 4$	0.690737714435067
$(0,6)$	$-1 \cdot 2^6 \cdot 3^5$	$x + 2$	1.01273471076020
$(0,7)$	$-1 \cdot 2^4 \cdot 3^3 \cdot 7^2$	$x - 2$	0.979250830047902
$(0,8)$	$-1 \cdot 2^{10} \cdot 3^3$	$x^2 + 8$	0.326617338771488
$(0,9)$	$-1 \cdot 2^4 \cdot 3^7$	$x + 2,\ x - 3,\ x - 6$	0.814695440566826

Table VI.2: Polynomials with lowest logarithmic Mahler measure for elliptic curves with Weierstrass equation $y^2 = x^3 + b$

Degree	**Polynomial(s)**	**Mahler measure***
1	$x+4, x+2$	1.05379074496120
2	x^2-4x-2	0.653234677542977
3	$x^3+12x+4$	0.577051381860239
4	$5x^4+8x^3-4x+8$	0.614584719192473
5	$x^5-4x^4+4x^3+16x^2+8x-8$	0.898284155037891
6	$x^6+2x^5-6x^4+6x^3-4x^2+8$	1.36234276093379
7	$x^7+2x^6-8x^4+16$	1.68540919397947
8	$x^8-x^7-4x^6-4x^5$ $-x^4+4x^3+4x^2+8$	2.59362671993106
9	$x^9+3x^7-4x^5+4x^3-16x^2-16$	4.11007180854945
10	$x^{10}+3x^9+4x^8+2x^7+$ $3x^6+10x^5+4x^4+4x^3+16$	5.08668079966427

Table VI.3: Gaussian search for elliptic curve with Weierstrass equation $y^2 = x^3 + 1$ with Discriminant $-1 \cdot 2^4 \cdot 3^3$. Time: 1-01:07:03

Degree	Polynomial(s)	Mahler measure*
1	$x + 4, x + 2$	1.05379074496120
2	$x^2 - 4x - 2$	0.653234677542977
3	$x^3 - 6x^2 - 6x - 8$	1.17503611100531
4	$5x^4 + 8x^3 - 4x + 8$	0.614584719192473
5	$2x^5 - 5x^3 + 2x^2 + 4$	1.42302578567335
6	$x^6 - 2x^5 - 2x^4 - 4x^3 +$ $4x^2 - 8x - 8$	1.32624570690264
7	$x^7 + 4x^6 + 24x^4 + 32x + 32$	2.06956324431806
8	$x^8 + 2x^7 - 4x^6 - 10x^5 +$ $8x^4 + 10x^3 - 20x^2 + 8$	5.03376271287971
9	$x^9 + 2x^8 + 2x^7 + 2x^6 +$ $6x^5 - 4x^4 + 16x^2 - 16$	3.99156422678977
10	$x^{10} + 6x^9 - 2x^8 + 4x^7 - 2x^6 - 40x^5$ $-40x^4 - 40x^3 + 16x^2 - 16x - 32$	3.86082372342556

Table VI.4: Uniform search for elliptic curve with Weierstrass equation $y^2 = x^3 + 1$ with Discriminant $-1 \cdot 2^4 \cdot 3^3$. Time: 2-04:32:56

Degree	**Polynomial(s)**	**Mahler measure***
1	$x-4, x-2$	1.05379074496120
2	x^2+2	0.326617338771488
3	x^3+2x^2-4x+4	0.577051381860240
4	x^4-2x^2+4 $x^4-4x^3+4x^2+8$	0.653234677542977
5	$x^5+6x^4-4x^3-4x^2-8$	0.657588342372568
6	$x^6+4x^5-4x^2+8$	1.31667811950241
7	$x^7+x^6+6x^5-5x^4+$ $4x^3+12x^2+4x+4$	3.05183384166068
8	$x^8-8x^7+2x^6+8x^5+8x^4+16$	2.53253563903305
9	$x^9-6x^8-12x^6+6x^5-16$	2.57182965677848
10	$x^{10}-x^9+x^8+x^7+3x^6-$ $4x^4+8x^2-16x+16$	5.15778836743889

Table VI.5: Polynomials with lowest Mahler measure* for elliptic curve with Weierstrass equation $y^2 = x^3 - 1$ with Discriminant $-1 \cdot 2^4 \cdot 3^3$

Degree	Polynomial(s)	Mahler measure*
1	$x+2, x-2$ $x+3, x-3$	1.77725174967924
2	x^2+2x+3 x^2-2x+3	0.888625874839619
3	x^3+x^2+5x+1	1.13231962601135
3	$2x^3+x^2-1$ $2x^3-x^2+1$	1.13231962601135
4	$x^4-4x^3-2x^2+4x-3$ $x^4+4x^3-2x^2-4x-3$	0.382595734777817
4	$3x^4+4x^3+2x^2-4x-1$ $3x^4-4x^3+2x^2+4x-1$	0.382595734777817
5	$x^5-2x^4+2x^3+x^2-x+1$	1.28710348399708
5	$x^5+x^4+x^3-2x^2-2x-1$	1.28710348399708

Table VI.6: Polynomials with lowest Mahler measure* for elliptic curve with Weierstrass equation $y^2 = x^3 - x$ with Discriminant 2^6

Degree	**Polynomial(s)**	**Mahler measure***
6	$x^6 + x^5 - x^4 - 6x^3 - x^2 + x + 1$ $x^6 - x^5 - x^4 + 6x^3 - x^2 - x + 1$	0.835556254585544
7	$x^7 - 4x^6 - 3x^5 - x^4 +$ $3x^3 + 2x^2 - x - 1$	1.30825680336215
8	$x^8 - x^7 + x^6 + x^5 -$ $8x^4 + x^3 + x^2 - x + 1$	2.74463318749962
9	$x^9 + x^8 - 6x^7 + 6x^6 - 6x^5 -$ $14x^4 - 14x^3 - 2x^2 + x + 1$	2.75313238735643
10	$x^{10} + x^8 - 9x^6 + 4x^5$ $-2x^4 + 4x^3 - 2x^2 - 1$	4.82659959985403

Table VI.7: Polynomials with lowest Mahler measure* for elliptic curve with Weierstrass equation $y^2 = x^3 - x$ with Discriminant 2^6

Degree	Polynomial(s)	Mahler measure*
1	$x+1$	0.0996167945961298
2	x^2-x+2	0.873715096613374
3	$5x^3-5x^2+3x+1$	0.855018198128853
4	$2x^4+x^3+x^2-x+1$	1.75820673708738
5	$x^5-x^4+6x^3+2x^2+x-1$	1.89498403507989
6	$x^6-2x^5-x^4+x^3+x^2+x+1$	3.09341169900270
7	$x^7-x^6+x^5+x^4-$ x^3-3x^2-x-1	3.11722188454591
8	x^8-x^3+x+1	4.09481812866632
9	$x^9+x^8-2x^7-3x^6+6x^5+$ $2x^4-12x^3-x^2-x+1$	5.80461187088794
10	$x^{10}+2x^9-x^8-5x^7+14x^6+$ $8x^5-x^4+11x^3-x^2+8x-4$	7.30912926994978

Table VI.8: Polynomials with lowest Mahler measure* for elliptic curve with Weierstrass equation $y^2=x^3-x-1$ with Discriminant $-1\cdot 2^4\cdot 23$

Chapter VII

FUTURE PLANS

An obvious next step in our study is to increase the number of elliptic curves to find results for. In particular, we would like to examine results when the linear and constant term range over $\{-9, \ldots, 9\}$. It would be interesting to examine what other effects, if any, negative values of a and b have on the canonical height.

Computing the canonical height can take a considerable amount of time. A natural bottleneck often involves integer factorization. Thus we restricted our polynomials to have degree 10 or lower. When working in the classical case one can use Wells' algorithm [25] to compute this height very quickly. Müller and Stoll [16] have demonstrated a similar algorithm which does this for elliptic curves over $\mathbb{Q}$ and more generally over arbitrary number fields.

An alternative way of approaching the height computation has been sought be using the dynamical height associated to Lattès map. This should also lead to quicker computations, and has the benefit of providing different Lattès maps to compute the height. It would be interesting to see how that affects the Mahler measure of our polynomials. In theory this can be done for elliptic curves over arbitrary number fields.

It may also be worth trying to set up an online database of heights of polynomials for different elliptic curves. Though this would require extra computational resources, the benefits may be worthwhile.

In this study we mostly used Gaussian and uniform random distributions to generate the coefficients for our polynomials. For future study we would like to investigate what effect other distributions would have on the speed of our genetic algorithm. We expect that in the limit as the degree of our polynomials go to infinity, the distribution should not have an effect on convergence. Thus choosing the right distribution may let us search much more quickly than before, with no sacrifices in robustness.

The polynomials in our study may be related to the torsion polynomials for our elliptic curves. We would also like to investigate the canonical measure on Berkovich space with respect to primes of bad reduction.

Going beyond the elliptic Lehmer conjecture, it may be worth asking if there is a way to formulate the Schnizel-Zassenhaus conjecture on elliptic curves and study polynomials in that context. It would also be intriguing to see results on the Chebyshev problem using genetic algorithms. Other aspects of machine learning would also be interesting to see applied to this rich field.

Bibliography

[1] Francesco Amoroso and Roberto Dvornicich, *A lower bound for the height in abelian extensions*, J. Number Theory **80** (2000), no. 2, 260–272. MR 1740514

[2] Matthew H. Baker, *Lower bounds for the canonical height on elliptic curves over abelian extensions*, Int. Math. Res. Not. (2003), no. 29, 1571–1589. MR 1979685

[3] Matthew H. Baker and Joseph H. Silverman, *A lower bound for the canonical height on abelian varieties over abelian extensions*, Math. Res. Lett. **11** (2004), no. 2-3, 377–396. MR 2067482

[4] José Ignacio Burgos Gil, Ricardo Menares, and Juan Rivera-Letelier, *On the essential minimum of Faltings' height*, Math. Comp. **87** (2018), no. 313, 2425–2459. MR 3802441

[5] Sinnou David and Marc Hindry, *Minoration de la hauteur de Néron-Tate sur les variétés abéliennes de type C. M*, J. Reine Angew. Math. **529** (2000), 1–74. MR 1799933

[6] Vesselin Dimitrov, *A proof of the schinzel-zassenhaus conjecture on polynomials*, (2019), Preprint available at `arXiv:1912.12545`.

[7] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. **34** (1979), no. 4, 391–401. MR 543210

[8] Graham Everest and Chris Pinner, *Bounding the elliptic Mahler measure. II*, J. London Math. Soc. (2) **58** (1998), no. 1, 1–8. MR 1666050

[9] ———, *Corrigendum: "Bounding the elliptic Mahler measure. II" [J. London Math. Soc. (2)* **58** *(1998), no. 1, 1–8; MR1666050 (2000a:11099)]*, J. London Math. Soc. (2) **62** (2000), no. 2, 640. MR 1783650

[10] Marc Hindry and Joseph H. Silverman, *On Lehmer's conjecture for elliptic curves*, Séminaire de Théorie des Nombres, Paris 1988–1989, Progr. Math., vol. 91, Birkhäuser Boston, Boston, MA, 1990, pp. 103–116. MR 1104702

[11] D. H. Lehmer, *Factorization of certain cyclotomic functions*, Ann. of Math. (2) **34** (1933), no. 3, 461–479. MR 1503118

[12] D. W. Masser, *Small values of the quadratic part of the Néron-Tate height on an abelian variety*, Compositio Math. **53** (1984), no. 2, 153–170. MR 766295

[13] Michael J Mossinghof, *Lehmer's problem*, `http://www.cecm.sfu.ca/~mjm/Lehmer/`.

[14] Michael J Mossinghoff, *Polynomials with small mahler measure*, Math. Comput. **67** (1998), 1697–1705.

[15] Michael J. Mossinghoff, Georges Rhin, and Qiang Wu, *Minimal Mahler measures*, Experiment. Math. **17** (2008), no. 4, 451–458. MR 2484429

[16] J. Steffen Müller and Michael Stoll, *Computing canonical heights on elliptic curves in quasi-linear time*, LMS J. Comput. Math. **19** (2016), no. suppl. A, 391–405. MR 3540967

[17] S. El Otmani, A. Maul, G. Rhin, and J.-M. Sac-Épée, *Finding new small degree polynomials with small mahler measure by genetic algorithms*, Rocky Mountain J. Math. **47** (2017), no. 8, 2619–2626.

[18] Clayton Petsche, Lucien Szpiro, and Thomas J. Tucker, *A dynamical pairing between two rational maps*, Trans. Amer. Math. Soc. **364** (2012), no. 4, 1687–1710. MR 2869188

[19] Robert Rumely, *On Bilu's equidistribution theorem*, Spectral problems in geometry and arithmetic (Iowa City, IA, 1997), Contemp. Math., vol. 237, Amer. Math. Soc., Providence, RI, 1999, pp. 159–166. MR 1710794

[20] R. Salem, *A remarkable class of algebraic integers. Proof of a conjecture of Vijayaraghavan*, Duke Math. J. **11** (1944), 103–108. MR 10149

[21] ______, *Power series with integral coefficients*, Duke Math. J. **12** (1945), 153–172. MR 11720

[22] Joseph H. Silverman, *A lower bound for the canonical height on elliptic curves over abelian extensions*, J. Number Theory **104** (2004), no. 2, 353–372. MR 2029512

[23] Joseph H. Silverman, *The arithmetic of dynamical systems*, Graduate Texts in Mathematics, no. 241, Springer, New York, 2007.

[24] C. J. Smyth, *On the product of the conjugates outside the unit circle of an algebraic integer*, Bull. London Math. Soc. **3** (1971), 169–175. MR 289451

[25] Elliot Wells, *Computing canonical heights on the projective line with no factorization*, Math. Comp. **86** (2017), no. 308, 3019–3029. MR 3667036

[26] Shou-Wu Zhang, *Equidistribution of small points on abelian varieties*, Ann. of Math. (2) **147** (1998), no. 1, 159–165. MR 1609518

APPENDIX

Tables

Table 1: Polynomials with lowest logarithmic Mahler measure for non-CM elliptic curves with Weierstrass equation $y^2 = x^3 + ax + b$

Elliptic Curve	Discriminant	Polynomial(s)	Mahler measure*
(1,1)	$-1 \cdot 2^4 \cdot 31$	$x^2 + 1$	0.363956108202543
(1,2)	$-1 \cdot 2^8 \cdot 7$	$x^3 + 9x^2 - x - 1$	0.674285680214076
(1,3)	$-1 \cdot 2^4 \cdot 13 \cdot 19$	$x + 1$	0.487827471310529
(1,4)	$-1 \cdot 2^6 \cdot 109$	$x + 1$	0.826064809404037
(1,5)	$-1 \cdot 2^4 \cdot 7 \cdot 97$	$x - 3$	1.30182743620374
(1,6)	$-1 \cdot 2^8 \cdot 61$	$x + 1$	0.145671950671431
(1,7)	$-1 \cdot 2^4 \cdot 1327$	$x - 1$	0.835698911788334
(1,8)	$-1 \cdot 2^6 \cdot 433$	$x + 1$	1.29251192618338
(1,9)	$-1 \cdot 2^4 \cdot 7 \cdot 313$	x	1.19468075763940

Continued on next page

Table 1 – continued from previous page

Elliptic Curve	**Discriminant**	**Polynomial(s)**	**Mahler measure***
(2,1)	$-1 \cdot 2^4 \cdot 59$	x $x^4 - 4x^2 - 8x + 4$	0.203459785486135
(2,2)	$-1 \cdot 2^6 \cdot 5 \cdot 7$	$x - 2$	0.684541945782354
(2,3)	$-1 \cdot 2^4 \cdot 5^2 \cdot 11$	$x^2 - 2x + 2$	0.394888972874392
(2,4)	$-1 \cdot 2^8 \cdot 29$	x	0.584786212715271
(2,5)	$-1 \cdot 2^4 \cdot 7 \cdot 101$	$x + 2$	0.721096332635923
(2,6)	$-1 \cdot 2^6 \cdot 251$	$x^2 - 2$	1.07342255153244
(2,7)	$-1 \cdot 2^4 \cdot 5 \cdot 271$	$x^2 - 2x + 6$	0.997775463972007
(2,8)	$-1 \cdot 2^9 \cdot 5 \cdot 11$	$x^2 - 4x + 6$	0.361297851884208
(2,9)	$-1 \cdot 2^4 \cdot 7 \cdot 317$	$x - 2$	1.15415566254717
(3,1)	$-1 \cdot 2^4 \cdot 3^3 \cdot 5$	$x^3 - 3x^2 + 3x - 5$ $x^3 - 6x^2 - 3x - 8$	0.218874210209203
(3,2)	$-1 \cdot 2^7 \cdot 3^3$	$x - 1$	0.518316137636907
(3,3)	$-1 \cdot 2^4 \cdot 3^3 \cdot 13$	$x^3 - 3x^2 + 3x + 3$	0.674694669890980
			Continued on next page

Table 1 – continued from previous page

Elliptic Curve	Discriminant	Polynomial(s)	Mahler measure*
(3,4)	$-1 \cdot 2^6 \cdot 3^3 \cdot 5$	$x^2 - 4x + 1$ $x^2 + 4x + 9$	0.473721235517371
(3,5)	$-1 \cdot 2^4 \cdot 3^3 \cdot 29$	$x - 1$	0.127766310765716
(3,6)	$-1 \cdot 2^7 \cdot 3^3 \cdot 5$	$x + 3$	0.713464935459064
(3,7)	$-1 \cdot 2^4 \cdot 3^3 \cdot 53$	$x + 1$	0.526003722366855
(3,8)	$-1 \cdot 2^6 \cdot 3^3 \cdot 17$	$x + 1$	0.791686648053312
(3,9)	$-1 \cdot 2^4 \cdot 3^3 \cdot 5 \cdot 17$	$x - 3$	0.358750811631971
(4,1)	$-1 \cdot 2^4 \cdot 283$	x	0.297727813465237
(4,2)	$-1 \cdot 2^6 \cdot 7 \cdot 13$	x	0.284784301337537
(4,3)	$-1 \cdot 2^4 \cdot 499$	$3x^2 + 4$	1.29436811808329
(4,4)	$-1 \cdot 2^8 \cdot 43$	x	0.281455622327844
(4,5)	$-1 \cdot 2^4 \cdot 7^2 \cdot 19$	$x^2 - 2x + 4$	0.604032113716847
(4,6)	$-1 \cdot 2^6 \cdot 307$	x	0.781218771242103
(4,7)	$-1 \cdot 2^4 \cdot 1579$	$3x^2 + 4$	1.41455991052718

Continued on next page

Table 1 – continued from previous page

Elliptic Curve	**Discriminant**	**Polynomial(s)**	**Mahler measure***
(4,8)	$-1 \cdot 2^{10} \cdot 31$	$x+2$	0.503378220000443
(4,9)	$-1 \cdot 2^{4} \cdot 7 \cdot 349$	x	0.743643777821825
(5,1)	$-1 \cdot 2^{4} \cdot 17 \cdot 31$	x^2-2x-1	1.04107702775509
(5,2)	$-1 \cdot 2^{9} \cdot 19$	$x-1$	0.451884263370590
(5,3)	$-1 \cdot 2^{4} \cdot 743$	$x-1$	0.781621345388887
(5,4)	$-1 \cdot 2^{6} \cdot 233$	$x+1$	0.992806524619626
(5,5)	$-1 \cdot 2^{4} \cdot 5^{2} \cdot 47$	x	1.04568486892598
(5,6)	$-1 \cdot 2^{10} \cdot 23$	x^2-2x+5	0.408316753352653
(5,7)	$-1 \cdot 2^{4} \cdot 1823$	$x+1$	0.741666628698170
(5,8)	$-1 \cdot 2^{6} \cdot 557$	$x+1$	1.22378868525625
(5,9)	$-1 \cdot 2^{4} \cdot 2687$	$x+1$	1.64887235907498
(6,1)	$-1 \cdot 2^{4} \cdot 3^{4} \cdot 11$	x	0.583566156735363
(6,2)	$-1 \cdot 2^{6} \cdot 3^{5}$	x^2+2	0.323222590746315
(6,3)	$-1 \cdot 2^{4} \cdot 3^{3} \cdot 41$	x	0.595091542146719

Continued on next page

Table 1 – continued from previous page

Elliptic Curve	**Discriminant**	**Polynomial(s)**	**Mahler measure***
(6,4)	$-1 \cdot 2^8 \cdot 3^4$	$x^2 - 4x - 2$	0.689862725980313
(6,5)	$-1 \cdot 2^4 \cdot 3^4 \cdot 19$	$x^2 + 2$	0.871608347758051
(6,6)	$-1 \cdot 2^6 \cdot 3^3 \cdot 17$	$x^2 + 2$	1.07167785676353
(6,7)	$-1 \cdot 2^4 \cdot 3^7$	$x^2 + 2$	0.539636932338589
(6,8)	$-1 \cdot 2^9 \cdot 3^4$	$x^2 + 4x + 10$	0.645414413814339
(6,9)	$-1 \cdot 2^4 \cdot 3^3 \cdot 113$	x	0.333990524334742
(7,1)	$-1 \cdot 2^4 \cdot 1399$	$x - 1$	0.718154053250788
(7,2)	$-1 \cdot 2^7 \cdot 5 \cdot 37$	$x - 1$	0.901613518782643
(7,3)	$-1 \cdot 2^4 \cdot 5 \cdot 17 \cdot 19$	$x + 1$	0.544316026258306
(7,4)	$-1 \cdot 2^6 \cdot 11 \cdot 41$	x	1.09463871192322
(7,5)	$-1 \cdot 2^4 \cdot 23 \cdot 89$	$x + 1$	1.34798617496802
(7,6)	$-1 \cdot 2^7 \cdot 293$	$x + 1$	1.58599523627637
(7,7)	$-1 \cdot 2^4 \cdot 5 \cdot 7^2 \cdot 11$	$x + 7$	0.867124857231287
(7,8)	$-1 \cdot 2^6 \cdot 5^2 \cdot 31$	$x^2 - 2x + 7$	0.900204889873143
			Continued on next page

Table 1 – continued from previous page

Elliptic Curve	Discriminant	Polynomial(s)	Mahler measure*
(7,9)	$-1 \cdot 2^4 \cdot 3559$	$x+1$	0.722575100052823
(8,1)	$-1 \cdot 2^4 \cdot 5^2 \cdot 83$	$x-2$	0.149802285871369
(8,2)	$-1 \cdot 2^6 \cdot 7^2 \cdot 11$	$x-4$	0.196055958528937
(8,3)	$-1 \cdot 2^4 \cdot 29 \cdot 79$	x	1.29757234151462
(8,4)	$-1 \cdot 2^8 \cdot 5 \cdot 31$	x	0.213291268155789
(8,5)	$-1 \cdot 2^4 \cdot 7 \cdot 389$	x	1.40470535221282
(8,6)	$-1 \cdot 2^6 \cdot 5 \cdot 151$	$x-2$	0.766958288348527
(8,7)	$-1 \cdot 2^4 \cdot 3371$	$x-1$	1.34137319142381
(8,8)	$-1 \cdot 2^{10} \cdot 59$	x	0.406919570972270
(8,9)	$-1 \cdot 2^4 \cdot 5 \cdot 7 \cdot 11^2$	x^2-6x+4	0.402880914919260
(9,1)	$-1 \cdot 2^4 \cdot 3^3 \cdot 109$	$x+1$	0.719493603425569
(9,2)	$-1 \cdot 2^8 \cdot 3^3 \cdot 7$	$x+5$	0.741398647425703
(9,3)	$-1 \cdot 2^4 \cdot 3^5 \cdot 13$	x^3-9x^2+9x+3	0.800919441714977
(9,4)	$-1 \cdot 2^6 \cdot 3^3 \cdot 31$	$x+1$	0.702485425092876

Continued on next page

Table 1 – continued from previous page

Elliptic Curve	**Discriminant**	**Polynomial(s)**	**Mahler measure***
(9,5)	$-1 \cdot 2^4 \cdot 3^3 \cdot 7 \cdot 19$	$x + 2$	1.15200710124834
(9,6)	$-1 \cdot 2^8 \cdot 3^5$	$x^2 + 3$	0.605471623688913
(9,7)	$-1 \cdot 2^4 \cdot 3^3 \cdot 157$	$x + 1$	1.04346125346854
(9,8)	$-1 \cdot 2^6 \cdot 3^3 \cdot 43$	$x - 1$	0.634391077495663
(9,9)	$-1 \cdot 2^4 \cdot 3^6 \cdot 7$	x	0.558065802859382

Degree	**Polynomial(s)**	**Mahler measure***
1	$x+5, x-5$ $x+1, x-1$	1.02580294042034
2	$3x^2+5$	1.00236478409436
3	x^3+3x^2-5x+5 x^3-3x^2-5x-5	1.57607328142842
4	$x^4+2x^3+6x^2-10x+5$	1.80652900096635
5	$x^5+2x^4+9x^3-x^2-5$	3.41173895718794
6	$x^6+4x^4+3x^3+5x-5$	6.37309223749437
7	$x^7+5x^6+3x^5+9x^4+$ $7x^3-9x^2+5x-5$	5.58831093638554
8	$x^8-2x^5-2x^4+8x^3-$ $4x^2+10x+5$	8.10788029582693
9	$x^9+2x^8-x^6-4x^5-5x^4-$ $8x^3+9x^2-5x-5$	10.2433915423107
10	$x^{10}+x^9+3x^8+5x^7-2x^6+$ $4x^5-6x^4+x^3+x^2+5x-5$	12.4577448770136

Table 2: Polynomials with lowest logarithmic Mahler measure for elliptic curve with Weierstrass equation $y^2 = x^3 + 5x$ and Discriminant $-1 \cdot 2^6 \cdot 5^3$

Degree	**Polynomial(s)**	**Mahler measure***
1	$x + 1$	0.809805254533880
2	$x^2 + 3$	0.906273466688998
3	$x^3 - 3x^2 + 3x + 3$	0.674694669890980
4	$x^4 - x^3 - 3x - 3$	1.92424930402729
5	$x^5 - 2x^4 - 5x^3 + 9x^2 + 6x + 3$	2.16339783289015
6	$x^6 - x^3 - 3x - 3$	3.58734628852022
7	$x^7 - 3x^5 + 3x^4 - 3x^3 + 9x + 9$	5.28277700862520
8	$x^8 - x^7 + 3x^6 + 5x^5 +$ $3x^3 - 3x^2 + 9x - 9$	5.60876338302969
9	$x^9 - x^8 - 5x^5 + 6x^4 - 6x^2 + 9$	8.61590478151529
10	$x^{10} + x^9 + 4x^8 + 7x^7 + 8x^6 +$ $10x^5 + 5x^4 + 5x^3 + 3x^2 - 3x - 3$	11.6191295072004

Table 3: Polynomials with lowest logarithmic Mahler measure for elliptic curve with Weierstrass equation $y^2 = x^3 + 3x + 3$ with Discriminant $-1 \cdot 2^4 \cdot 3^3 \cdot 13$

VITA

John Michael Clark

Candidate for the Degree of

Master of Science

Thesis: POLYNOMIALS WITH SMALL ELLIPTIC MAHLER MEASURE VIA GENETIC ALGORITHMS

Major Field: Mathematics

Biographical:

Education:

Completed the requirements for the Master of Science in Mathematics at Oklahoma State University, Stillwater, Oklahoma in May, 2020.

Completed the requirements for the Bachelor of Science in Mathematics at California Institute of Technology, Pasadena, California in 2016.

Professional Membership:

American Mathematical Society, Mathematical Association of America