The Conditional Probability that an Elliptic Curve has a Rational Subgroup of Order 5 or 7

Meagan Kenney
Advisor: John Cullinan

February 10, 2020

Elliptic Curves

Definition

An **elliptic curve** E over a field K, denoted E/K, is a projective, non-singular algebraic curve of genus 1 that contains an additional K-rational point. Equivalently, the equation for E/K is given by

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1}$$

such that $a_1, a_2, a_3, a_4, a_6 \in \bar{K}$ along with $\mathcal{O}$, the point at infinity.

Elliptic Curves

Remark

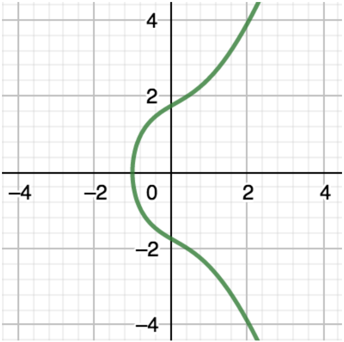
It is important to know that given an elliptic curve $E/\mathbf{Q}$ defined by the equation

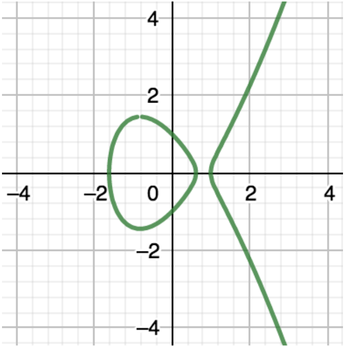
$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

we can actually conclude that $a_1, a_2, a_3, a_4, a_6 \in \mathbf{Z}$. This will be an important facet to many of our computations.

Elliptic Curves

- The possible solutions on an elliptic curve E are dependent on the field over which one is looking for solutions.
- Given an elliptic curve E, graphing $E(\mathbf{R})$ will always result in a curve of either one or two components that will resemble one of the two images below:





Equations of Elliptic Curves

Definition

An elliptic curve E/K given by the equation

$$E : y^2 = x^3 + Ax + B,$$

with $A, B \in \bar{K}$ is said to be in **short Weierstrass form.**

Equations of Elliptic Curves

Algorithm

Let E/K be an elliptic curve over K where $\mathrm{char}(K) \neq 2, 3$, given by the equation

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

Define

$$b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6,$$
$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$$
$$c_4 = b_2^2 - 24b_4, \quad c_6 = -b_2^3 + 36b_2b_4 - 216b_6.$$

From these substitutions we get that $E : y^2 = x^3 + Ax + B$, where $A = -27c_4$ and $B = -54c_6$.

Equations of Elliptic Curves

Definition

Given E in short Weierstrass form defined by the equation of the form

$$E : y^2 = x^3 + Ax + B,$$

then the **discriminant** of E is denoted $\Delta(E)$ and given by

$$\Delta(E) = -16(4A^3 + 27B^2).$$

Height

Note that given an elliptic curve $E/\mathbf{Q}$ we can obtain an equation for E in what is called short Weierstrass form through a simple change of variables

$$E : y^2 = x^3 + Ax + B,$$

with $A, B \in \mathbf{Z}$.

Definition

Let E be an elliptic curve given by the equation

$$E : y^2 = x^3 + Ax + B.$$

Then the **height** of E, denoted $\operatorname{ht} E$, is defined by the equation

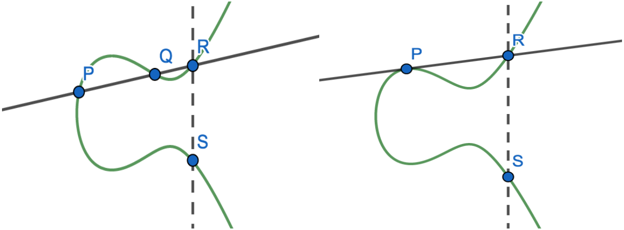
$$\operatorname{ht} E := \max(|4A^3|, |27B^2|).$$

The Group Law

Bézout's Theorem

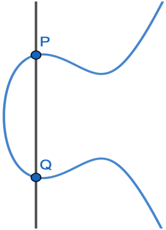
Given two curves C_1 and C_2 of degree m and n, respectively, the sum of the multiplicities at each of the points of the intersection of C_1 and C_2 is equal to mn.

Let E be an elliptic curve. Let P and Q be points on an elliptic curve.



The Group Law

- Note that $P \oplus \mathcal{O} = \mathcal{O} \oplus P$ for all points P on our elliptic curve. So the point at infinity $\mathcal{O}$ will serve as an identity on the set of points on an elliptic curve under point addition.
- Then the inverse of a point P on an elliptic curve is the point on the elliptic curve intersected by the vertical line going through P.



- This point addition is also associative, though that explanation is more complicated.

Torsion Points

- The set of points on an elliptic curve under the binary operation defined by this point “addition” form an abelian group.
- It is important to note that this point “addition” can be described algebraically by rational functions on the coordinates of the points being added.
- We may wish to add a point to itself numerous times. We will denote this

$$[m]P = \underbrace{(P \oplus P \oplus \cdots \oplus P)}_{m \text{ summands}}.$$

Torsion Points

Definition

Given a point $P \in E$, suppose that $\ell[P] = \mathcal{O}$ for some $\ell \in \mathbf{Z}$, then we say that the point P is a **torsion point** of E. If $[m]P \neq \mathcal{O}$ for all $m \in \mathbf{N}$ such that $0 < m < \ell$, then we say that P has order ℓ and also call P an ℓ-**torsion point**.

Definition

The set of all torsion points on E over $\mathbf{Q}$, is called the **torsion subgroup of** E and is denoted $E(\mathbf{Q})_{\mathrm{tor}}$.

- This structure of this subgroup will play a large role in determining the structure of $E(\mathbf{Q})$, the set of all rational points on an elliptic curve E.
- If an elliptic curve E has an ℓ-torsion point then $\ell | \# E(\mathbf{Q})_{\mathrm{tor}}$.

Torsion Points

Theorem (Mazur)

Let E be an elliptic curve over $\mathbf{Q}$. Then the torsion subrgoup of $E(\mathbf{Q})$ will have one of the following structures

$$E(\mathbf{Q})_{\text{tor}} \cong \mathbf{Z}/n\mathbf{Z} \text{ such that } 1 \leq n \leq 10 \text{ or } n = 12$$

$$E(\mathbf{Q})_{\text{tor}} \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2n\mathbf{Z} \text{ such that } n = 1, 2, 3, 4.$$

Nagell-Lutz Theorem

Given an elliptic curve $E/\mathbf{Q}$ in the form $E : y^2 = x^3 + Ax + B$, then if $P \in E(\mathbf{Q})_{\text{tor}}$ and $P = (x, y)$, we get that $x, y \in \mathbf{Z}$ and either $y = 0$, in which case P is a finite point of order 2, or y divides the discriminant of the curve E.

Local Divisibility

Reduction Modulo p Theorem

Let $E/\mathbf{Q}$ be an elliptic curve given by the equation

$$E : y^2 = x^3 + Ax + B.$$

Let $\Delta(E)$ be the discriminant of E. Let

$$\widehat{E} : y^2 = x^3 + \widehat{A}x + \widehat{B}$$

where $A \equiv \widehat{A} \pmod{p}$ and $B \equiv \widehat{B} \pmod{p}$. Then reduction modulo p map with $E(\mathbf{Q})_{tors}$ as its domain is a isomorphism that maps $E(\mathbf{Q})_{tors}$ to a subgroup of $\widehat{E}(\mathbf{F}_p)$ provided that $p \nmid \Delta(E)$.

Local Divisibility

Definition

Let E be an elliptic curve, if $\ell | \# E(\mathbf{F}_p)$ for all but finitely many primes p, we say that E has **local ℓ-divisibility.**

- Note then since for good primes p our reduction modulo p isomorphism maps $E(\mathbf{Q})_{tors}$ to a subgroup of $E(\mathbf{F}_p)$ then by Lagrange's Theorem $\# E(\mathbf{Q})_{tors} | \# E(\mathbf{F}_p)$.
- Therefore if $\ell | \# E(\mathbf{Q})_{tors}$ then $\ell | \# E(\mathbf{F}_p)$.
- Therefore ℓ-torsion implies local ℓ-divisibility

The Question

- We have shown that ℓ-torsion implies local ℓ-divisibility; however, the converse only holds up to isogeny.

Theorem (Katz)

Given an elliptic curve E with local ℓ-divisibility, there exists a curve E' that is isogenous to E, such that E' has ℓ-torsion.

Theorem (Cullinan and Voight)

Given an elliptic curve E with local m-divisibility, the probability P_m that $E(\mathbf{Q})$ has m-torsion is non-zero for all m allowed by Mazur's classification of rational torsion on elliptic curves.

Question

Given $\ell = 5$ or $\ell = 7$ and an elliptic curve E with local ℓ-divisibility, what is the probability that E has ℓ-torsion?

Key Ideas For Counting Curves

- Consider parameterizations of curves with each desired structure that can be found using standard techniques.
- Order curves by height.
- Sieve out non-minimal equations.
- Apply the Principle of Lipschitz to compact regions containing coordinate pairs that correspond to a unique minimal elliptic curve with the desired structure.

Tate Normal Form

Theorem (Tate)

Let $m \in \{4, 5, 6, 7, 8, 9, 10, 12\}$. The **Tate normal form** of an elliptic curve E with a torsion point of order m is given by the equation

$$E = E(b, c) : y^2 + (1 - c)xy - by = x^3 - bx^2,$$

where the polynomial conditions that must be satisfied by b and c are determined by the exact value of m.

- Let E be an elliptic curve in Tate Normal From with m-torsion. Suppose P is the point of order m on E. Then by the construction of the Tate normal form we get that $P = (0, 0)$.

Parameterizations

- Given that $P = (0, 0)$ consider the following calculations of points.

$$P = (0,0), \quad 2P = (b, bc), \quad 3P = (c, b - c),$$

$$4P = \left(\frac{b}{c}\left(\frac{b}{c} - 1\right), \left(\frac{b}{c}\right)^2 \left(c - \frac{b}{c} + 1\right) \right),$$

$$-P = (0, b), \quad -2P = (b, 0), \quad -3P = (c, c^2),$$

$$-4P = \left(\frac{b}{c}\left(\frac{b}{c} - 1\right), \frac{b}{c}\left(\frac{b}{c} - 1\right)^2 \right).$$

- If we would like P to be a point of 5-torsion on our elliptic curve it must be the case that $P = -4P$, $2P = -3P$, $3P = -4P$, and $4P = -P$.

Parameterizations

- We actually can get our polynomial values of b and c by just comparing one pair of points.
- Setting $2P$ equal to $-3P$ yields $(b, bc) = (c, c^2)$.
- Thus we can conclude that given an elliptic curve E in Tate Normal Form

$$E = E(b, c) : y^2 + (1 - c)xy - by = x^3 - bx^2,$$

  that E has 5-torsion when $b = c$.
- Therefore from Tate we get that an elliptic curve with a point of order 5 can be given by the following general equation in Tate Normal form

$$E : y^2 + (1 - t)xy - ty = x^3 - tx^2$$

  for some $t \in \mathbf{Q}$.

Parameterizations

Rewriting this equation to get the short Weierstrass form, we get that for $t \in \mathbf{Q}$, the general equation for a curve E over $\mathbf{Q}$ with a point of order 5 is given by the equation

$$E : y^2 = x^3 + f(t)x + g(t),$$
$$f(t) = -27c_4 = -27t^4 + 324t^3 - 378t^2 - 324t - 27,$$
$$g(t) = -54c_6 = 54t^6 - 972t^5 + 4050t^2 + 972t + 54.$$

We would like an integral model. So we set $t = \frac{a}{b}$ for some $a, b \in \mathbf{Z}$ to get the following integral model for the general equation of an elliptic curve E with a point of order 5:

$$y^2 = x^3 + A(a,b)x + B(a,b),$$
$$A(a,b) = -27a^4 + 324a^3b - 378a^2b^2 - 324ab^3 - 27b^4,$$
$$B(a,b) = 54a^6 - 972a^5b + 4050a^4b^2 + 4050a^2b^4 + 972ab^5 + 54b^6.$$

Isogenies

Definition

Given two elliptic curves E_1 and E_2, a morphism $\phi : E_1 \to E_2$ such that $\phi(\mathcal{O}) = \mathcal{O}$ is called an **isogeny**.

Definition

Two elliptic curves E_1 and E_2 are **isogenous** if there exists a nonzero isogeny $\phi : E_1 \to E_2$.

For example, let $m \in \mathbf{Z}$. Consider the *multiplication-by-m map* defined by $[m] : E \to E$ such that

$$m(P) = \begin{cases} P \oplus P \oplus \cdots \oplus P, & \text{if } m > 0 \\ (-P) \oplus (-P) \oplus \cdots \oplus (-P), & \text{if } m < 0 \\ \mathcal{O} & \text{if } m = 0. \end{cases}$$

Isogenies

Theorem

Isogenies are well-defined modulo all but finitely many primes.

Theorem

Let $E_1/\mathbf{F}_p$ and $E_2/\mathbf{F}_p$ be elliptic curves. Then E_1 and E_2 are isogenous over $\mathbf{F}_p$ if and only if

$$\#E_1(\mathbf{F}_p) = \#E_2(\mathbf{F}_p).$$

Isogenies

Theorem

Let E_1 and E_2 be elliptic curves such that the curve E_1 has local m-divisibility. Suppose that E_1 is isogenous to E_2, then E_2 also has local m-divisibility.

- This follows from the fact that if E_1 and E_2 are isogenous curves, then they are isogenous over the finite field $\mathbf{F}_p$ for all but finitely many primes p.
- Therefore for all but finitely many primes p we get that $\#E_1(\mathbf{F}_p) = \#E_2(\mathbf{F}_p)$.

Isogenies

Corollary

Let E_1 and E_2 be isogenous elliptic curves and let ϕ be the nonzero isogeny between them then $\ker \phi$ is a finite subgroup of E_1.

Theorem

Given an elliptic curve E and F, a finite subgroup of E, there exists a unique elliptic curve E' and a separable isogeny ϕ where

$$\phi : E \to E' \quad \text{satisfies } \ker \phi = F.$$

Often the curve satisfying these properties is denoted E/F.

Vélu's Algorithm

- Let E be an elliptic curve in Tate normal form with a point of order 5. Recall then that E is given by the equation
$$E : y^2 + (1-t)xy - ty = x^3 - tx^2, \tag{2}$$
for some $t \in \mathbf{Q}$.
- To compute the desired isogenous curve we follow Vélu's Algorithm.
- Let $F = \{P, 2P, 3P, 4P, \mathcal{O}\}$, that is F is a subgroup of $E(\mathbf{Q}(t))_{\mathrm{tor}}$ generated by P which is a point of order 5 on E due to the fact that E is in the Tate normal form.
- Let $R = \{P, 2P\}$, then $-R = \{3P, 4P\}$, and note that this then satisfies the proper conditions that every point in R has its inverse in $-R$, and $R \cup (-R) = F - \{\mathcal{O}\}$ and $R \cap (-R) = \emptyset$.

Vélu's Algorithm

- To follow the algorithm of Vélu to get an isogenous curve to our parameterized curve with 5-torsion, set

$$a_1 = 1 - t, \quad a_2 = -t, \quad a_3 = -t, \quad a_4 = 0, \quad a_6 = 0,$$

which are simply the coefficients of E.

- Vélu's Algorithm then gives us that our isogenous curve $\widehat{E}$ over F is given by the equation

$$\widehat{E} : y^2 + a_1xy + a_3y = x_3 + a_2x^2 + (a_4 - 5T)x + (a_6 - b_2T - 7W),$$

where

$$T = \sum_{Q \in R} t_Q, \quad W = \sum_{Q \in R} (u_Q + x_Q t_Q)$$

and t_Q and u_Q are simply formulas involving the x-coordinate of the point Q.

Parameterization

- Calculating T and W yields the following parameterization of elliptic curves that by construction will have local 5-divisibility without 5-torsion:

$$\widehat{E} : y^2 + (1-t)xy - ty = x_3 - tx^2$$

$$+(-5t^3-10t^2+5t)x+(-t^5-10t^4+26t^3-57t^2+22t).$$

- So we get the following integral universal model for elliptic curves with local 5-divisibility, without 5-torsion:

$$y^2 = x^3 + \widehat{A}(a,b)x + \widehat{B}(a,b),$$

$$\widehat{A}(a,b) = -27a^4 - 6156a^3b - 13338a^2b^2 + 6156ab^3 - 27b^4.$$

$$\widehat{B}(a,b) = 54a^6 - 28188a^5b - 540270a^4b^2$$

$$- 540270a^2b^4 + 28188ab^5 + 54b^6.$$

Isomorphic Elliptic Curves

Definition

Let E_1 and E_2 be elliptic curves. Then E_1 is **isomorphic** to E_2, denoted $E_1 \cong E_2$, when there exists morphisms $\phi : E_1 \to E_2$ and $\psi : E_2 \to E_1$ such that

$$\psi \circ \phi = \mathbf{1}_{E_1} \text{ and } \phi \circ \psi = \mathbf{1}_{E_2}.$$

- Given E_1/K and E_2/K, we say E_1 is isomorphic to E_2 over K if ϕ and ψ as defined above can be defined over K.
- Note that two elliptic curves defined by equations in short Weierstrass form are isomorphic if and only if they satisfy a certain change of variables that can be defined by an invertible morphism.

Isomorphic Elliptic Curves

The unique change of variables of the equation for E that results in another Short Weierstrass equation of an isomorphic elliptic curve is given by

$$x = u^2 x' \quad \text{and} \quad y = u^3 y',$$

which results in

$$u^4 A' = A, \quad u^6 B' = B, \quad u^{12} \Delta'(E') = \Delta(E),$$

which yields the equation of the isomorphic elliptic curve

$$E' : y^2 = x^3 + A' x^2 + B'.$$

Isomorphic Elliptic Curves

Definition

Given an elliptic curve E defined by the equation

$$E : y^2 = x^3 + Ax + B,$$

then the j-**invariant** is given by the formula

$$j(E) = \frac{-1728(4A)^3}{\Delta(E)}.$$

Proposition

Two elliptic curves E_1 and E_2 are isomorphic if and only if $j(E_1) = j(E_2)$.

Minimal Models

- Note that in $\mathbf{Q}$, in order to send $x \to u^2x'$ and $y \to u^3y'$ requires that $u^2|x$ and $u^3|y$.
- Thus eventually we will get to an elliptic curve given by the equation $\widehat{E} : y^2 = x^3 + \widehat{A}x^2 + \widehat{B}$ such that $u^2 \nmid \widehat{A}$ and $u^3 \nmid \widehat{B}$ for all possible values of $u \in \mathbf{Z}$.

Definition

Let E/K be an elliptic curve, and let $\Delta(E)$ be the discriminant of E. Then the Weierstrass equation that defines E is called a **minimal model** if and only if $p^{12} \nmid \Delta(E)$ for all primes p.

Our Regions

Define the region:

$$R_5(X) = \left\{(a,b) \in \mathbf{R}^2 \mid |A(a,b)| \leq \left(\frac{X}{4}\right)^{(1/3)} \text{ and } |B(a,b)| \leq \left(\frac{X}{27}\right)^{(1/2)}\right\}.$$

Define the region:

$$\widehat{R}_5(X) = \left\{(a,b) \in \mathbf{R}^2 \mid |\widehat{A}(a,b)| \leq \left(\frac{X}{4}\right)^{(1/3)} \text{ and } |\widehat{B}(a,b)| \leq \left(\frac{X}{27}\right)^{(1/2)}\right\}.$$

Our Regions

Proposition

The Principle of Lipschitz states that the area of a compact region is equal to the number of integral points in the region plus a small error term.

- We will use the Principle of Lipschitz to obtain a count for the number of points in each of our regions $R_5(X)$ and $\widehat{R}_5(X)$.

Proposition

The regions $R_5(X)$ and $\widehat{R_5}(X)$ are homogenous such that

$$Area(R_5(X)) = X^{1/6}Area(R_5(1))$$

$$Area(\widehat{R_5}(X)) = X^{1/6}Area(\widehat{R_5}(1))$$

The Count and the Probability

- Let $N_5(X)$ denote our count of isomorphism classes of elliptic curves up to height X with 5-torsion, and let $\widehat{N}_5(X)$ denote our count of isomorphism classes of elliptic curves up to height X with local 5-divisibility without 5-torsion.
- Note that by definition

$$P_5 = \lim_{X \to \infty} \frac{N_5(X)}{N_5(X) + \widehat{N}_5(X)}.$$

Sieving

Using a combinatorial sieve altered from a method used by Harron and Snowden we sieve out the non-minimal models of elliptic curves corresponding to each prime number less than or equal to $X^{1/12}$ to get that

$$N_5(X) = \frac{Area(R_5(1))}{\zeta(2)} X^{1/6} + O(X^{1/12}),$$

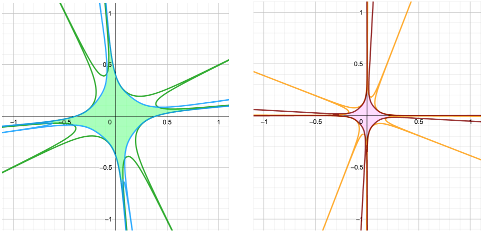
$$\widehat{N}_5(X) = \frac{Area(\widehat{R}_5(1))X^{1/6}}{\zeta(2)} + O(X^{1/12}),$$

which implies that

$$P_5 = \frac{Area(R_5(1))}{Area(R_5(1)) + Area(\widehat{R}_5(1))}.$$

Comparing Areas

Consider the graphs of $R_5(1)$ and $\widehat{R}_5(1)$



We performed a simple rotation and reflection of $\widehat{R}_5(X)$ to obtain the following:

Theorem

We can show that

$$Area(R_5(X)) = 5 \cdot Area(\widehat{R}_5(X)).$$

Comparing Areas

Theorem

We can show that

$$Area(R_5(X)) = 5 \cdot Area(\widehat{R}_5(X)).$$

- Let $\theta = \frac{1}{2}\arctan(\frac{2}{11})$.
- Then
$$\hat{A}(x\cos\theta - y\sin\theta, -(x\sin\theta + y\sin\theta)) = A(\sqrt{5}x, \sqrt{5}y).$$
- Similarly
$$\hat{B}(x\cos\theta - y\sin\theta, -(x\sin\theta + y\sin\theta)) = B(\sqrt{5}x, \sqrt{5}y).$$

Results for P_5

- Recall that from using sieving methods from Harron and Snowden we have concluded that

$$P_5 = \frac{Area(R_5(1))}{Area(R_5(1)) + Area(\widehat{R}_5(1))}.$$

- Combining this with the previous theorem we have that

$$Area(R_5(1)) = 5 \cdot Area(\widehat{R}_5(1)),$$

which implies that

$$P_5 = \frac{5Area(\widehat{R}_5(1))}{5Area(\widehat{R}_5(1)) + Area(\widehat{R}_5(1))} = \frac{5}{6}.$$

Theorem (CK, 2019)

We have that $P_5 = \frac{5}{6}$.

Considering P_7

- To compute P_7 we can mirror the methods we used to make our universal models for P_5 to make models with 7-torsion and local 7-divisibility, without 7-torsion.
- The strategy breaks down when sieving and attempting to find an angle of rotation to compare the area of our regions.
- Despite this we use experimental data to make the following conjecture that

$$P_7 = \frac{\sqrt{7}}{1+\sqrt{7}}.$$

Bibliography

[1] J. Cullinan and J. Voight, *On a probabilistic local-global principle for torsion on elliptic curves*, In preparation.

[2] I. Garcia-Selfa, M. A Olalla, and J. M. Tornero, *Computing the Rational Torsion of an Elliptic Curve Using Tate Normal Form*, Journal of Number Theory **96** (2002), 76-88.

[3] R. Harron and A. Snowden, *Counting Elliptic Curves with Prescribed Torsion*, Crelles Journal **729** (2017), 151-170.

[4] M. Hindry and J. H. Silverman, *Diophantine Geometry: An Introduction*, Springer-Verlag New York, 2000.

[5] D. Husemöller, *Elliptic Curves, Second Edition*, New York: Springer Verlag, 2004.

[6] International GeoGebra Institute, *GeoGebra Graphing Calculator (Version 6.0.528)*, 2019, `http://www.geogebra.org`.

[7] N. Katz, *Galois properties of torsion points on abelian varieties*, Inventiones Mathematicae **62** (1981), 481-502.

[8] N Koblitz, *Introduction to Elliptic Curves and Modular Forms, Second Edition*, New York: Springer Verlag, 1993.

[9] The LMFDB Collaboration, *The L-functions and Modular Forms Database*, 2013, `http://www.lmfdb.org`.

[10] J. H. Silverman, *The Arithmetic of Elliptic Curves, Second Edition*, New York: Springer-Verlag, 2009.

[11] J. H. Silverman and John Tate, *Rational Points on Elliptic Curves*, Springer-Verlag New York, 1992.

[12] W. Stein, *SageMath, the Sage Mathematics Software System (Version 8.4)*, 2018, `http://www.sagemath.org/`.

[13] J. Vélu, *Isogénies entre courbes elliptiques*, Comptes Renus de l'Académie des Sciences des Paris **273** (1971), 238–241.