Zeros of the Modular Parametrization of Rational Elliptic Curves

A thesis submitted to the Department of Mathematics of the University of Hawai'i in partial fulfillment of Plan B for the Master's Degree in Mathematics.

November 18, 2011

By

Lisa Kodgis

Thesis Committee:

Dr. Pavel Guerzhoy, Chairman

Dr. Xander Faber

Graduate Committee:

Dr. J. B. Nation, Graduate Chair

Dr. Robert Little

Dr. Michelle Manes

Dr. George Wilkens

Acknowledgments

I would like to thank my advisor, Pavel Guerzhoy, for an education, and for doing so with an inspiring passion for mathematics. Also I would like to thank Professors Robert Little, Heiner Dovermann, and Dale Myers for their mentorship along the way and Professor Ron Brown for his insightful algebra lectures. I thank my mother for her love and support through the years.

ZEROS OF THE MODULAR PARAMETRIZATION OF RATIONAL ELLIPTIC CURVES

LISA KODGIS

ABSTRACT. Some Rational elliptic curves whose modular parametrization is given by an Eichler integral were considered. The points, other than cusps, that map to zero under modular parametrization were studied computationally. Surprisingly, these zeros appear to be CM-points.

This paper is organized under the following section headings:

1991 *Mathematics Subject Classification.* Primary 11F11 ; Secondary 14H52 .

1. Introduction

This exposition explains a numerical experiment, which involved finding zeros of Eichler integrals. The background will provide definitions and basic information about cusp forms and elliptic curves, and how the Eichler integral is a well-defined map between a modular curve and an elliptic curve. Then, we address the question of which points under this map are zeros on the elliptic curve with a computational experiment.

2. Background Information

2.1. **Elliptic Curves.**

The first collection of objects of interest in this paper will be rational elliptic curves. We will follow the description given in [2]. For $a_i \in \mathbb{Q}$, these coefficients come from the following projective curve

$$(1)\quad E\ :\ F(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3.$$

The projective cubic E is an *elliptic curve* if its discriminant $\Delta(E)$ is non-zero. In order to define the quantity $\Delta(E)$, put

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= a_1a_3 + 2a_4 \\ b_6 &= a_3^2 + 4a_6 \\ b_8 &= b_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \end{aligned}$$

and let

$$\Delta(E) = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6.$$

For a field k the set of k-points of E is

$$E(k) = \{(x:y:z) \in \mathbb{P}^2(k) | F(x,y,z) = 0\}.$$

In particular, for a prime p, and $k = \mathbb{F}_p = \mathbb{Z}/pZ$, we see that set $E(\mathbb{F}_p)$ is finite, and we denote its cardinality by $\#E(\mathbb{F}_p)$. The condition $\Delta(E) \neq 0$ becomes $\Delta(E) \not\equiv 0 \bmod p$. We thus call the prime p *good* if $p \nmid \Delta(E)$, and *bad* if $p | \Delta(E)$. There are obviously only finitely many bad primes for a given elliptic curve E. The property of a prime p to be good for E translates into the fact that the *reduction* of the elliptic curve modulo p is an elliptic curve over the finite field $\mathbb{F}_p$. For bad primes, we call the reduction *degenerate*.

Note that the cardinality of a projective line over $\mathbb{F}_p$ is $p+1$, and, for good primes p, consider the difference

$$a(p) := p + 1 - \#E(\mathbb{F}_p).$$

We expand this definition of $a(p)$ for primes p to $a(n)$ for integers $n \geq 1$ by the requirement that the Dirichlet series $L_E(s) := \sum a(n)n^{-s}$ (which is called the L-function of the elliptic curve E) has the following Euler product decomposition

$$L_E(s) = \sum_{n=1}^{\infty} \frac{a(n)}{n^s} = \prod_{p \nmid \Delta(E)} \frac{1}{1 - a(p)p^{-s} + p^{1-s}} \prod_{p | \Delta(E)} \frac{1}{1 - a(p)p^{-s}},$$

where, for bad primes p, $a(p)$ takes the value of either ±1 or 0, which depends on certain properties of the reduction $E(\mathbb{F}_p)$.

2.2. **Cusp Forms.** Now we change our focus to begin to define the other main object of cusp forms. First, let us consider the following special linear group

$$SL_2(\mathbb{Z}) = \left\{ \left(\begin{array}{cc} a & b \\ c & d \end{array} \right) | a, b, c, d \in \mathbb{Z} \text{ and } ad - bc = 1 \right\},$$

where the operation is matrix multiplication. The group $SL_2(\mathbb{Z})$ acts on the upper-half (complex) plane, $\mathbb{H} = \{\tau | \tau \in \mathbb{C} \text{ and } Im(\tau) > 0\}$ in the following way, for $\gamma = \left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \in SL_2(\mathbb{Z})$ and $\tau \in \mathbb{H}$, we have

$$\gamma\tau = \left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \tau = \frac{a\tau + b}{c\tau + d}.$$

We will be interested in subgroups of $SL_2(\mathbb{Z})$ of the form

$$\Gamma_0(N) = \left\{ \left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \in SL_2(\mathbb{Z}) | c \equiv 0 (\text{mod } N) \right\}.$$

The group $\Gamma_0(N)$ acts on the set $\mathbb{H}^* := \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$.

Now let $f : \mathbb{H} \to \mathbb{C}$ be a holomorphic function that transforms under the action of $\Gamma_0(N)$ in the following way

$$f(\gamma\tau) = f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^2 f(\tau) \text{ for all } \gamma = \left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \in \Gamma_0(N). \tag{2}$$

Since $\left(\begin{array}{cc} 1 & 1 \\ 0 & 1 \end{array} \right) \in \Gamma_0(N)$ for every N, the condition (2) implies, in particular, that f must be periodic, and, therefore, has a Fourier expansion

$$f(q) = \sum_n c(n) q^n \text{ where } q = e^{2\pi i \tau}.$$

We impose some extra requirements that f is holomorphic, and approach zero at every cusp, which are elements of the set $\mathbb{Q} \cup \{\infty\}$. At the cusp of infinity this condition translates to the requirement that the coefficients $c(n)$ vanish for $n \leq 0$. We refer to the holomorphic functions which satisfy the transformation law (2) and this extra requirement at cusps as *cusp forms of weight* 2 *and level* N and we denote the linear space of these functions by $S_2(N)$.

The L-series of a cusp form is significantly easier to find compared to an elliptic curve, for a cusp form $f(z) = \sum_{n=1}^{\infty} c(n) q^n$, the L-series is simply

$$L_f(s) = \sum_{n=1}^{\infty} c(n) n^{-s}$$

for $s \in \mathbb{C}$.

Clearly, if $f \in S_2(N)$, then $f \in S_2(MN)$ for any positive integer M. A cusp form $f \in S_2(N)$ is called *new* if its level is exact, namely $f \notin S_2(N/M)$ for all integers $M \geq 2$. A cusp form $f \in S_2(N)$ is called a primitive Hecke eigenform if it is new, $c(1) = 1$ (normalized), and its L-series has an Euler product decomposition

$$L_f(s) = \sum_{n=1}^{\infty} \frac{c(n)}{n^s} = \prod_{p|N} \frac{1}{1 - c(p)p^{-s}} \prod_{p \nmid N} \frac{1}{1 - c(p)p^{-s} + p^{1-s}}.$$

The finite dimensional linear space (over $\mathbb{C}$) $S_2(N)$ has a basis which consists of normalized Hecke eigenforms.

2.3. **The Main Theorem.** The connection between the L-series of modular forms and elliptic curves was explored as early as the 1950s when Yutaka Taniyama conjectured that the L-series of elliptic curve over $\mathbb{Q}$ coincides with the L series of a weight 2 normalized newform for $\Gamma_0(N)$. One implication of this conjecture was proven in the 1960s by Martin Eichler and Goro Shimura.

Theorem 2.1 (Eichler-Shimura Congruence Relation)**.** *Let $f = \sum_{n=1}^{\infty} a(n)q^n \in S_2(N)$ be primitive Hecke eigenform. If $a(n) \in \mathbb{Z}$, then there exists a rational elliptic curve E such that $L_E(s) = L_f(s)$.*

The level N of the form f in the theorem becomes the *conductor* of the elliptic curve E, which may be calculated as the product of certain powers of bad primes. Conversely, Andrew Wiles' famous theorem (which implies Fermat's Last Theorem) tells us that every rational elliptic curve can be produced from a primitive weight two Hecke eigenform in this way.

The difficult part of the Eichler-Shimura Congruence Relation theorem is the coincidence of L-series, while the elliptic curve associated with a primitive Hecke eigenform f by the theory of Eichler and Shimura can be constructed quite explicitly as follows. This procedure is known as *modular parametrization.*

We will follow [4]. Begin with the Eichler integral,

$$\phi(\tau) = 2\pi i \int_{\tau}^{i\infty} f(\tau')\ d\tau' = -\sum_{n=1}^{\infty} \frac{a(n)}{n} q^n$$

The derivative of the Eichler integral is $\phi' = -2\pi i f dz$, where $f = \sum_{n=1}^{\infty} a(n)q^n \in S_2(N)$.

For $\gamma\tau,\ \tau \in \mathbb{H}$ let us consider the difference $\frac{d}{d\tau}(\phi(\gamma\tau) - \phi(\tau))$. By modularity, $f\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^2 f(\tau)$ and by the quotient rule, $\left(\frac{a\tau+b}{c\tau+d}\right)' = \frac{1}{(c\tau+d)^2}$, the difference is then $-2\pi i \left((c\tau+d)^2 f(\tau)\frac{1}{(c\tau+d)^2} - f(\tau)\right) = 0$.

Since this difference is zero, we see that $C(\gamma) := \phi(\gamma\tau) - \phi(\tau)$ is a constant for all $\gamma \in \Gamma_0(N)$. We thus obtain a map $C : \Gamma_0(N) \to \mathbb{C}$. This map becomes a group homomorphism if $\mathbb{C}$ is considered as an additive group, and easily follows from $C(\gamma) = \int_{\gamma\tau}^{\tau} f(\tau')\ d\tau'$.

Since $C\ :\ \Gamma_0(N) \to \mathbb{C}$ is a group homomorphism, its image is a subgroup in $\mathbb{C}$. It is known that this is a rank two discrete subgroup, and therefore can be realized as a lattice Λ.

The quotient $\mathbb{C}/\Lambda$ is thus a smooth projective curve of genus one, therefore an elliptic curve, and we know that is specifically the rational elliptic curve describe in Eichler-Shimura and that if we let

$$g_2 = 60 \sum_{\omega\in\Lambda,\ \omega\neq 0} \frac{1}{\omega^4}, \quad \text{and} \quad g_3 = 140 \sum_{\omega\in\Lambda,\ \omega\neq 0} \frac{1}{\omega^6}.$$

Then the quantities g_2 and g_3 are rational numbers, and the equation of a rational elliptic curve

$$y^2 = 4x^3 - g_2 x - g_3$$

which can be transformed by a standard variable change procedure to a minimal equation of the form (1).

2.4. **A question about the map ϕ.** The map ϕ constructed in the previous section is known as *modular parametrization*. Namely, ϕ is a map from $\mathbb{H}^*$ to $\mathbb{C}/\Lambda$ which factors through the action of $\Gamma_0(N)$ on $\mathbb{H}^*$. Indeed, if $\tau_1 = \gamma(\tau_2)$, then the difference between their images $\phi(\tau_1) - \phi(\tau_2) \in \Lambda$. We therefore have a well-defined, holomorphic map

$$\phi \ : \ \mathbb{H}^*/\Gamma_0(N) \to \mathbb{C}/\Lambda$$

from a modular curve, $\mathbb{H}^*/\Gamma_0(N)$, to an elliptic curve. The importance and fundamental nature of this map attracted lots of attention to it. However, not too much is known. It is known that the map surjects (is a covering). In general, ϕ is not an isomorphism. In order to show that, it suffices to observe that while the genus of $E = \mathbb{C}/\Lambda$ is one, the genus of $\mathbb{H}^*/\Gamma_0(N)$ grows with N roughly as $N/12$, and is equal to one only for finitely many values of N. Thus the degree of the map $\deg \phi > 1$ for almost all N. (There is no standard formula to calculate $\deg \phi$ since the genus of the target is one. However the degree was calculated by Zagier [4] in the case when N is a prime, and this calculation has been expanded to the general case by Cremona [1].) Several authors have addressed the question about where on the modular curve under the map ϕ are the ramification points. No definite results are obtained, but it is observed by Oda [3] that in many cases ramification happens when the point is a CM-point. A point τ in the upper half plane is called a CM-point if there exist integers a,b, and c with $a \neq 0$ such that $a\tau^2 + b\tau + c = 0$. We address a simpler question here. The map ϕ is set up so that $\phi(i\infty) = 0$. It may also happen that other cusps map to the points in Λ. (It is known that cusps always map to division points, that is for every cusp c there is an integer M_c such that $M_c\phi(c) \in \Lambda$.) Still, since $\deg \phi$ may be quite large, there may be points $\tau \in \mathbb{H}$ in the interior of the upper half-plane such that $\phi(\tau) \in \Lambda$. The question about these points reduces to solving the equation

$$\phi(\tau) = 0$$

for τ.

3. The Experiment

The computation was performed using *gp* [5]. Zeros of each Eichler integral were found by approximating the infinite sum as a polynomial.

$$\phi = \sum_{n=1}^{k} \frac{c(n)}{n} q^n$$

where $q = e^{2\pi i \tau}$. Curves were chosen for which the degree of the Eichler integral was known to be greater than 1. We will explain the code in terms of a particular elliptic curve $y^2 + xy = x^3 - x^2 - 10x - 12$, which is represented as $[1, -1, 0, -10, -12]$. First we test to find possible roots

$\backslash p$ 400

$lim = 400;$

$E = [1, -1, 0, -10, -12];$

$E = ellinit(E, flag = 0);$

$Ef = sum(n = 1, lim, ellak(E, n)/n * q\hat{\ }n);$

$z = polroots(Ef);$

$for(i = 1, length(z), N = norm(z[i]); if(N < .9, print(i, "...", N)));$

The first line in the code set the decimal precision to 400 digits. The second line is our parameter for the degree of the polynomial, which was done uniformly at 400 for all elliptic curves tested. The line $E = [1, -1, 0, -10, -12];$ is where we specify the elliptic curve. In the next line $E = ellinit(E, flag = 0);$ gives the elliptic curve its structure.

We approximate the Eichler integral as polynomial of degree *lim* in the line $Ef = sum(n = 1, lim, ellak(E, n)/n * q^n);$, where the function $ellak(E, n)$ computes coefficients of the L-series for the elliptic curve. This sum is in terms of $q = e^{2\pi i\tau}$. Then $z = polroots(Ef);$ calculates the roots of this polynomial.

The last step of the code is a *for* loop that assigns a number to each root of this polynomial and if the norm, the complex modulus, of this root is less than the value of 0.9, then it prints the enumeration, and the norm. As we want the sum to converge, the norm must be less than 1, and sufficiently far from 1 for faster convergence, so the value 0.9 was chosen.

For this particular example, $[1, -1, 0, -10, -12]$, where the second series of "..." signifies that we cut off our decimals at 20 digits from the original 400, we get the following information.

2...0.$E - 809$

79...0.72069902083393305312...

80...0.72069902083393305312...

The degree of this map is known to be 5, one of the roots must and does have norm of 0, this is the cusp ∞. We also see that we have two possible roots of the same norm. Each $z[i]$ is the i^{th} root, expressed in terms of q, so we find the complex number τ in the following way

$tau = log(z[79])/(2 * Pi * I)$

This gives the result, displaying only 20 of the 400 digits.

$0.12500000000000000000\ldots + 0.026064301757134345 33\ldots * I$

For this particular example, it appears that the real part is $\frac{1}{8}$. We then try to determine is if the imaginary part is rational as well by considering it as a continued fraction. Let us recall that a continued fraction is a fraction of the form

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{a_4 + \cdots}}}}$$

where the $a_i \in \mathbb{Z}$. In order for a continued fraction to represent a rational number, the above representation must stop at some point.

In *gp*, the function $contfrac$ considers the argument as a continued fraction in this form, and returns $[a_0, a_1, a_2, a_3, \ldots]$, where the length of the output depends on the nature of the number and set precision. For $contfrac(1/8)$ we get $[0, 8]$ as expected.

We use the code $contfrac(imag(tau))$, which (again we cut off) returns

$$[0, 38, 2, 1, 2, 1, 2, 76, 2, 1, 2, 1, 2, 76, 2, 1, 2, 1, 2, 76, 2, 1, 2, 1, 2, 76, 2, 4, 2, 1, 1, 1, \ldots]$$

From this representation (including the omitted part) we do not see a reason why this would be a rational number, but we do notice something else, particularly a pattern. This pattern suggests that this number is quadratic.

As it is likely a quadratic we then consider the continued fraction of the square of this number, $contfrac(imag(tau)^2)$, which gives

$$[0, 1472, 125250061933692041598551736, 1, 2, \ldots].$$

The large third number suggests that this is rational and so we convert this to a fraction by using $contfracpnqn([0, 1472, 125250061933692041598551736])$, which gives $\frac{1}{1472}$, and as we took the square initially, we see that the imaginary part is likely $\sqrt{\frac{1}{1472}}$.

As for the other possible root with the same norm, we resolve it into its real and imaginary components to get

$$-0.12500000000000000000\ldots + 0.02606430175713434533\ldots * I,$$

so the other possible root is the same, but with negative real part.

Now that we have two possible roots, let us see if it is likely that the series converges at these points. We test this with the following sequence of code

$E = [1, -1, 0, -10, -12];$

$E = ellinit(E, flag = 0);$

$Ef = sum(n = 1, 1000, ellak(E, n)/n * exp(2 * n * Pi * I * (1/8 + I/sqrt(1472))))$

Which gives a value that is approximately zero, $-8.49\ldots E^{-74} - 2.95\ldots E^{-74} * I$, and finally around 10000 terms, it is $-1.62\ldots E^{-405} + 6.08\ldots E^{-406} * I$, which is beyond our precision. Indeed, the Eichler integral converges rapidly.

4. Results

Below is a table summarizing zeros that were found of the 269 Eichler integrals examined. The first column is the conductor of the elliptic curve and level of the cusp form, the second column is the elliptic curve, the third column lists the degree of the map, which gives an upper bound on number of zeros, and the last column lists the zeros found. Note that if $\phi(q) = 0$, then $\phi(\bar{q}) = 0$. Thus, since $q = e^{2\pi i\tau}$, the τ-roots of ϕ come in pairs $\tau = \pm a + bi$. Also, this method found the cusp ∞ as root for all of the 269 curves, but this method excludes considering the other cusps $\mathbb{Q}$ because their norm is 1. We list below the zeros that have positive real part and are in $\mathbb{H}$.

Conductor	Elliptic Curve	Degree	Roots
46	[1,-1,0,-10,-12]	5	$\frac{1}{8} + \frac{i}{8\sqrt{23}}$
63	[1,-1,0,9,0]	4	$\frac{17}{42} + \frac{i}{42\sqrt{3}}$
67	[0,1,1,-12,-21]	5	$\frac{1}{2} + \frac{i}{2\sqrt{67}}$
75	[0,-1,1,-8,-7]	6	$\frac{1}{2} + \frac{i}{10\sqrt{3}}$
85	[1,1,0,-8,-13]	4	$\frac{26}{85} + \frac{2i}{85}$
99	[1,-1,0,-15,8]	12	$\frac{7}{18} + \frac{i}{18\sqrt{11}}$
99	[0,0,1,-3,-5]	6	$\frac{1}{2} + \frac{i}{6\sqrt{11}}$
106	[1,0,0,1,1]	6	$\frac{23}{53} + \frac{i}{53}$
106	[1,1,0,-27,-67]	10	$\frac{1}{6} + \frac{i}{6\sqrt{53}}$
109	[1,-1,0,-8,-7]	4	$\frac{43}{109} + \frac{2i}{109}$
110	[1,1,1,10,-45]	20	$\frac{13}{30} + \frac{i}{30\sqrt{11}}$
115	[0,0,1,7,-11]	10	$\frac{1}{2} + \frac{i}{2\sqrt{115}}$
116	[0,1,0,-4,4]	8	$\frac{17}{116} + \frac{i}{116}, \frac{41}{116} + \frac{i}{116}$
118	[1,1,1,-4,-5]	6	$\frac{18}{59} + \frac{i}{59\sqrt{2}}$
118	[1,1,0,56,-192]	38	$\frac{1}{6} + \frac{i}{6\sqrt{59}}$
121	[1,1,1,-30,-76]	6	$\frac{3}{14} + \frac{i\sqrt{3}}{154}$
121	[1,1,0,-2,-7]	6	$\frac{38}{121} + \frac{2i\sqrt{2}}{121}$
121	[0,-1,1,-40,-221]	24	$\frac{1}{2} + \frac{i}{22}$
123	[0,1,1,-10,10]	20	$\frac{1}{6} + \frac{i}{6\sqrt{41}}$
126	[1,-1,0,-36,-176]	32	$\frac{1}{8} + \frac{i}{24\sqrt{7}}$
135	[0,0,1,-27,-115]	36	$\frac{1}{2} + \frac{i}{6\sqrt{15}}$
139	[1,1,0,-3,-4]	6	$\frac{39}{139} + \frac{2i\sqrt{2}}{139}$
141	[0,1,1,-12,2]	28	$\frac{1}{6} + \frac{i}{6\sqrt{47}}$
141	[0,1,1,-26,-61	12	$\frac{1}{2} + \frac{i}{2\sqrt{141}}$
142	[1,-1,1,-12,15]	36	$\frac{1}{2} + \frac{i}{2\sqrt{71}}$
142	[1,-1,0,-1,-3]	9	$\frac{1}{8} + \frac{i}{8\sqrt{71}}$
147	[0,1,1,-114,473]	42	$\frac{1}{2} + \frac{i}{14\sqrt{3}}$
147	[0,-1,1,-2,-1]	6	$\frac{1}{2} + \frac{i}{14\sqrt{3}}$
150	[1,1,1,37,281]	48	$\frac{4}{9} + \frac{i}{45\sqrt{2}}$
153	[1,-1,0,-6,-1]	8	$\frac{7}{17} + \frac{i}{51}$
153	[0,0,1,-27,-61]	24	$\frac{1}{2} + \frac{i}{6\sqrt{17}}$

Conductor	Elliptic Curve	Degree	Roots
158	[1,-1,1,-9,9]	32	$\frac{1}{2} + \frac{i}{2\sqrt{79}}$
158	[1,1,1,1,1]	6	$\frac{47}{158} + \frac{i\sqrt{3}}{158}$
163	[0,0,1,-2,1]	6	$\frac{46}{163} + \frac{i\sqrt{3}}{163}$
170	[1,-1,0,-10,-10]	20	$\frac{1}{5} + \frac{i}{5\sqrt{34}}$
171	[0,0,1,177,1035]	96	$\frac{1}{2} + \frac{i}{6\sqrt{19}}$
171	[0,0,1,-21,-41]	32	$\frac{1}{2} + \frac{i}{6\sqrt{19}}, \frac{1}{5} + \frac{i}{15\sqrt{19}}$
174	[1,1,1,-5,-7]	10	$\frac{13}{29} + \frac{i}{29\sqrt{6}}$
174	[1,0,1,0,-2]	52	$\frac{1}{8} + \frac{i}{8\sqrt{87}}$
174	[1,1,0,-56,-192]	8	$\frac{1}{8} + \frac{i}{8\sqrt{87}}$
175	[0,-1,1,2,-2]	8	$\frac{1}{14} + \frac{i\sqrt{3}}{70}$
175	[0,1,1,42,-131]	40	$\frac{1}{2} + \frac{i}{10\sqrt{7}}$
178	[1,0,0,6,-28]	32	$\frac{34}{89} + \frac{i}{89}$
178	[1,1,0,-44,80]	28	$\frac{1}{6} + \frac{i}{6\sqrt{89}}$
179	[0,0,1,-1,-1]	9	$\frac{72}{179} + \frac{i\sqrt{7}}{179}, \frac{1}{6} + \frac{i}{6\sqrt{179}}, \frac{1}{2} + \frac{i}{2\sqrt{179}}$
182	[1,-1,1,3,-5]	36	$\frac{5}{21} + \frac{i}{21\sqrt{26}}, \frac{2}{7} + \frac{i}{7\sqrt{26}}$
184	[0,0,0,-55,-157]	24	$\frac{1}{5} + \frac{i}{10\sqrt{46}}, \frac{3}{10} + \frac{i}{10\sqrt{46}}$
185	[0,-1,1,-5,6]	8	$\frac{14}{37} + \frac{i}{37\sqrt{10}}$
185	[1,0,1,-4,-3]	6	$\frac{86}{185} + \frac{2i}{185}$
186	[1,0,1,-17,-28]	28	$\frac{9}{62} + \frac{i\sqrt{5}}{62\sqrt{3}}$
187	[0,0,1,7,1]	30	$\frac{1}{2} + \frac{i}{2\sqrt{187}}$
189	[0,0,1,-6,3]	12	$\frac{5}{14} + \frac{i}{42\sqrt{3}}$
189	[0,0,1,-27,-7]	36	$\frac{1}{2} + \frac{i}{6\sqrt{21}}$
190	[1,-1,1,-48,147]	88	$\frac{1}{2} + \frac{i}{2\sqrt{95}}$
194	[1,-1,1,-3,-1]	14	$\frac{31}{194} + \frac{3i}{194}, \frac{\pm 71}{194} + i\frac{\sqrt{3}}{194}$
195	[0,1,1,0,-1]	12	$\frac{1}{2} + \frac{i}{2\sqrt{195}}$
195	[0,1,1,-66,-349]	84	$\frac{1}{2} + \frac{i}{2\sqrt{195}}$
195	[0,-1,1,-190,1101]	84	$\frac{1}{2} + \frac{i}{2\sqrt{195}}$
197	[0,0,1,-5,4]	10	$\frac{24}{197} + i\frac{\sqrt{15}}{197}$

5. Conclusions

1. The most surprising fact is that in *many* cases the zeros of ϕ turn out to be at CM-points. In fact, in most of the cases when our numerical experiments do not confirm that, we can find a reasonable explanation why the code is inadequate to these cases. For instance, for the curve $[0, 0, 1, -1, 0]$ of conductor $N = 37$, one can prove that no zeroes in $\mathbb{H}$, the interior of the upper half-plane, occur. In another case of the curve $[1, 0, 1, -7705, 1226492]$ of conductor $N = 174$ the degree of the modular parametrization is 1540; there is probably a zero of a multiplicity too big to retrieve it with our experiments.

Our experiments thus suggest a question quite similar to that suggested in Oda's survey [3] whether the zeros of ϕ in the interior of $\mathbb{H}$ are always at CM-points. (Oda asks the same question about the zeros of ϕ', the derivative of ϕ.) Additional computations suggest that the CM-points found here are not ramification points.

2. One can see by inspection of the above table that the zeros of ϕ are tightly related with the conductor N of the elliptic curve. Since the conductor was not directly involved into our experiments, this observation may be taken as an indirect confirmation of the correctness of our data. At the same time one can try to make this relation with the conductor quite precise. Specifically, let τ be a CM-point such that $\phi(\tau) = 0$, and let $\mathcal{N}(\tau) = \tau\overline{\tau} \in \mathbb{Q}$ be its Galois norm. Within the range of our experiments we observe that the denominator of the rational number $N\mathcal{N}(\tau)$ has no prime factors other than 2 and 3:

$$N\mathcal{N}(\tau) \in \mathbb{Z}_p \quad \text{for } p > 3.$$

Note that the numerator of $N\mathcal{N}(\tau)$ is never divisible by N within the range of our calculations. We would like to conjecture that this is always the case.

References

[1] J.E. Cremona, *Computing the Degree of the Modular Parametrization of a modular elliptic curve*, Mathematics of Computation, Volume 64, Number 211, (1995), 1235–1250.

[2] J.S. Milne, *Elliptic Curves, BookSurge Publishers, 2006.*

[3] T. Oda, The Birch and Swinnerton-Dyer Conjecture*, Sugaku Expositions, Volume 22, Number 2, (2009), 169–186.*

*[4] D. Zagier,*Modular Points, Modular Curves, Modular Surfaces and Modular Forms*, Lecture Notes in Mathematics, Volume 1111/1985, (1985), 225–248.*

[5] http://pari.math.u-bordeaux.fr/