MATHEMATICS OF COMPUTATION
Volume 83, Number 285, January 2014, Pages 411–420
S 0025-5718(2013)02709-3
Article electronically published on May 6, 2013

MINIMAL POLYNOMIALS OF SINGULAR MODULI

ERIC ERRTHUM

This paper is dedicated to my wife Kate.

Abstract. Given a properly normalized parametrization of a genus-0 modular curve, the complex multiplication points map to algebraic numbers called singular moduli. In both cases there are known algorithms for algebraically computing the rational norms of the singular moduli without relying on the the recognition of a decimal or p-adic expansion as a rational number. We demonstrate a method of extending these norm algorithms to determine the minimal polynomial of the singular moduli below a discriminant threshold. We then use these minimal polynomials to compute the algebraic *abc*-ratios for the singular moduli.

1. Introduction

The classical j-function is a modular function that has been studied since the late 1800s by the likes of Gauss, Hermite, Dedekind and Klein. Its values in the upper half-plane correspond to isomorphism classes of elliptic curves and at points corresponding to CM curves, the values of the j-function are called singular moduli. A Shimura curve is a generalization of the classical modular curve. Again there is a notion of singular moduli and in both cases singular moduli are algebraic numbers. Singular moduli have been computed using analytic methods [1] and in some cases [3] they have been computed algebraically. In this paper, we present a strictly algebraic method for determining the defining polynomials for a large class of singular moduli (both classical and Shimura) utilizing pre-existing algorithms that output their rational norms. It is worth noting that our method never relies on the recognition of a decimal or p-adic expansion as a rational number. This method works for singular moduli whose degree is strictly less than the number of rational singular moduli on the curve.

For instance, on the classical modular curve we compute that

$$j\left(\frac{1}{2}(1+i\sqrt{39})\right) = -\frac{27}{2}\left(6139474+1702799\sqrt{13}+147\sqrt{39\left(89453213+24809858\sqrt{13}\right)}\right).$$

Perhaps more importantly, we also compute minimal polynomials of singular moduli on the Shimura curve of discriminant 6. For example, the minimal polynomial of

Received by the editor November 14, 2010 and, in revised form, October 25, 2011 and May 2, 2012.

2010 *Mathematics Subject Classification.* Primary 11G18; Secondary 11Y40.

the singular modulus of discriminant 244 is

$$x^3 - \frac{2^2 3^7 31 \cdot 67 \cdot 37223 \cdot 235849}{17^6 29^6} x^2 + \frac{2^4 3^{14} 151 \cdot 1187 \cdot 163327}{17^6 29^6} x - \frac{2^6 3^{21} 19^4}{17^6 29^6}.$$

In Section 2 we give a brief review of modular curves both in the classical and Shimura cases. In Section 3 we review the Gross-Zagier formula for the algebraic norm of the difference of two singular moduli and demonstrate how it can be used to algebraically determine the minimal polynomial for a finite collection of singular moduli. In Section 4 we adapt this method to the Shimura curve defined by the quaternion algebra of discriminant 6. As suggested in [8], singular moduli have the potential to be good examples related to the *abc*-conjecture, so in Section 5 we review the basics for computing the algebraic *abc*-ratio and present the unencouraging data obtained from the singular moduli in both cases. Finally, in Section 6 we discuss the limitations of the method and ways to potentially overcome them.

Computations for this paper were performed in Mathematica (v7.0.1.0) and MAGMA (v2.13-14) provided by [12].

2. Modular curves and Singular Moduli

In this section we provide the basics of modular curves and singular moduli. For the purposes of this paper, we ignore level considerations. For a more complete description of these concepts, see [10], [16], [17], [18].

The classical modular curve $\mathcal{X}_1^*$ is the one-point compactification of the Riemann surface $\mathrm{GL}_2(\mathbb{Z})\backslash\mathfrak{h}^{\pm}$ where $\mathfrak{h}^{\pm} = \mathbb{P}^1(\mathbb{C}) - \mathbb{P}^1(\mathbb{R})$. As $\mathcal{X}_1^*$ is a surface of genus 0, it is isomorphic to $\mathbb{P}^1$. Since any map $j : \mathcal{X}_1^* \to \mathbb{P}^1$ must be invariant under the $\mathrm{GL}_2(\mathbb{Z})$ action, it suffices to define the function by giving its values at three points. In the classical setting, the points $i = \sqrt{-1}$, $\omega = \frac{1+i\sqrt{3}}{2}$, and ∞ are chosen to be sent to 1728, 0, and ∞, respectively. This choice yields what is now commonly referred to as the j-function and it has a known Fourier series expansion (where $\mathbf{q} = e^{2\pi i\tau}$):

$$j(\tau) = \frac{1}{\mathbf{q}} + 744 + 196884\mathbf{q} + \cdots \in \frac{1}{\mathbf{q}}\mathbb{Z}[[\mathbf{q}]].$$

The points of $\mathcal{X}_1^*$ correspond to isomorphism classes of elliptic curves. Some of these classes support an extra endomorphism and are called CM curves. Hence, the corresponding points on $\mathcal{X}_1^*$ are called CM points. In the classical case, the CM points of $\mathcal{X}_1^*$ are the imaginary roots of quadratic equations. When τ is a CM point, $j(\tau)$ is called a singular moduli and is an algebraic integer.

A Shimura curve is a generalization of the modular curve. Let B be the indefinite quaternion algebra over $\mathbb{Q}$ with discriminant $D > 1$ and let $\Gamma^* = N_{B^\times}(\mathcal{O}) \subset B^\times$ be the normalizer of a maximal order $\mathcal{O} \subset B$. Since there is an algebra embedding $B \hookrightarrow \mathrm{M}_2(\mathbb{R})$, the discrete group Γ^* embeds into $\mathrm{GL}_2(\mathbb{R})$ and hence acts on $\mathfrak{h}^{\pm}$. The Shimura curve $\mathcal{X}_D^*$ is then given as

$$\mathcal{X}_D^* = \Gamma^*\backslash\mathfrak{h}^{\pm}.$$

When B is a division algebra, $\mathcal{X}_D^*$ is a compact Riemann surface without cusps [11].

Points on a Shimura curve can be identified with certain 2-dimensional abelian varieties and again there is the notion of CM points. As in the case of the modular curve, one may normalize a generator for the function field, $t : \mathcal{X}_D^* \to \mathbb{P}^1$, such that the images of CM points under the generator are all algebraic over $\mathbb{Q}$. However,

since $\mathcal{X}_D^*$ has no cusps, such a map does not have a $\mathbf{q}$-expansion and calculations are more difficult than in the classical case.

3. Minimal polynomials of classical singular moduli

Let τ_1 and τ_2 be CM points on $\mathcal{X}_1^*$ with relatively prime negative discriminants $-d_1$ and $-d_2$. Let $h(-d_i)$ be the class number of the quadratic order of discriminant $-d_i$. If $-d_1$, $-d_2 < -4$, then $j(\tau_1) - j(\tau_2)$ is an algebraic integer over $\mathbb{Q}$ of degree $h(-d_1)h(-d_2)$. Let ω_i be the number of roots of unity in that order. Recall that in general the norm of an algebraic number is given by

$$|\alpha|_{\mathbb{Q}} = \prod_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})} \sigma(\alpha).$$

The main result of [10] is that the norm $|j(\tau_1) - j(\tau_2)|_{\mathbb{Q}}$ is given by

$$|j(\tau_1) - j(\tau_2)|_{\mathbb{Q}}^{\frac{2}{\omega_1 \omega_2}} = \pm \prod_{\substack{x, n, n' \in \mathbb{Z} \\ n, n' > 0 \\ x^2 + 4nn' = d_1 d_2}} n^{\epsilon(n')} \tag{1}$$

where $\epsilon(p)$ is a completely multiplicative function defined on primes p with $\left(\frac{d_1 d_2}{p}\right) \neq 1$ by

$$\epsilon(p) = \begin{cases} \left(\frac{-d_1}{p}\right) & \text{if } \gcd(p, -d_1) = 1, \\ \left(\frac{-d_2}{p}\right) & \text{if } \gcd(p, -d_2) = 1. \end{cases}$$

The computational benefit of (1) is that very little actually needs to be known about the algebraic integers $j(\tau_i)$ to perform the calculation.

We now proceed to describe our algorithm for computing the minimal polynomials of singular moduli. Suppose that $r \in \mathbb{Q}$ and τ is a CM point with discriminant $-d$. Then $\mathbb{Q}(r - j(\tau)) = \mathbb{Q}(j(\tau))$. Let $G = \mathrm{Gal}(\mathbb{Q}(j(\tau))/\mathbb{Q})$. Then

$$\begin{aligned} |r - j(\tau)|_{\mathbb{Q}} &= \prod_{\sigma \in G} \sigma(r - j(\tau)) \\ &= \prod_{\sigma \in G} r - \sigma(j(\tau)) \\ &= M_{j(\tau)}(r) \end{aligned}$$

where $M_\alpha(x) \in \mathbb{Q}[x]$ denotes the minimal polynomial of the algebraic number α.

Since the degree of $M_{j(\tau)}(r)$ is $h(-d)$, it suffices to know the value of the left-hand-side for $h(-d) + 1$ values of r to interpolate the polynomial. Hence, we only need to find $h(-d)+1$ rational $j(\tau_i)$ with $\gcd(d_i, d) = 1$ and then use (1) to find (up to an issue of sign which we discuss in the example below) the value of $M_{j(\tau)}(j(\tau_i))$.

Unfortunately, the number of rational singular moduli is finite: they occur exactly at the CM points of discriminants -4, -8, -3, -7, -11, -19, -43, -67, and -163. This fact limits the previous method to only being possible for singular moduli of degree 8 or less. The largest achievable case is the singular moduli of discriminant -5923.

Also, it should be noted that this algorithm is in no way optimal or the most efficient from a computational viewpoint. Many of these facts can be discovered through much quicker analytic, floating-point calculations and the recognition of

approximations. The importance of our method lies in its purely algebraic nature. This, in turn, allows it it be implemented in the Shimura curve case, as we will see in Section 4.

3.1. **Example:** $j(\frac{1}{2}(1+i\sqrt{39}))$**.** Fix $\tau = \frac{1}{2}(1+i\sqrt{39})$. Then $d = 39$ and $h(-d) = 4$. Since $-d$ is relatively prime to the discriminants -4, -8, -7, -11, and -19, we can use (1) to compute the following:

$$\begin{aligned}
|j(\tau) - j(1+i)| &= 3^{12}7^8 19^4 23^2, \\
|j(\tau) - j(1+i\sqrt{2})| &= 7^8 13^2 23^2 29 \cdot 31^2 37^2 53, \\
|j(\tau) - j(\tfrac{1}{2}(1+i\sqrt{7}))| &= 3^{12}7^4 13^2 17^3 19^2 31^2, \\
|j(\tau) - j(\tfrac{1}{2}(1+i\sqrt{11}))| &= 7^8 13^2 17^3 19^2 29^2 101 \cdot 107, \\
|j(\tau) - j(\tfrac{1}{2}(1+i\sqrt{19}))| &= 3^{12}13^2 19^2 29 \cdot 31^2 37^2 \cdot 53 \cdot 113 \cdot 173 \cdot 179.
\end{aligned}$$

This gives the following 5 points on the curve $y = |M_{j(\tau)}(x)|$:

$$\begin{aligned}
(x_1, y_1) &= (12^3,\ 3^{12}7^8 19^4 23^2), \\
(x_2, y_2) &= (20^3,\ 7^8 13^2 23^2 29 \cdot 31^2 37^2 53), \\
(x_3, y_3) &= (-15^3,\ 3^{12}7^4 13^2 17^3 19^2 31^2), \\
(x_4, y_4) &= (-32^3,\ 7^8 13^2 17^3 19^2 29^2 101 \cdot 107), \\
(x_5, y_5) &= (-96^3,\ 3^{12}13^2 19^2 29 \cdot 31^2 37^2 \cdot 53 \cdot 113 \cdot 173 \cdot 179).
\end{aligned}$$

Since the absolute value obscures the polynomial's outputs, we fall back on an exhaustive search through the 16 different possibilities of choices for the signs of the y_i. Then using standard curve fitting we find that only one choice of signs, namely

$$(x_1, y_1),\ (x_2, y_2),\ (x_3, -y_3),\ (x_4, -y_4),\ (x_5, -y_5),$$

yields a monic polynomial. It is

$$\begin{aligned}
M_{j(\tau)}(x) &= x^4 + 331531596x^3 - 429878960946x^2 + 109873509788637459x \\
&\quad + 20919104368024767633 \\
&= x^4 + 2^2 3^3 11 \cdot 29 \cdot 9623x^3 - 2 \cdot 3^6 41 \cdot 1303 \cdot 5519x^2 \\
&\quad + 3^{12}103 \cdot 2007246533x + 3^{15}17^3 23^3 29^3.
\end{aligned}$$

Since this is only a degree 4 polynomial over the reals, it is solvable by radicals and yields 4 roots. By comparing these to decimal approximations for $j(\tau)$ computed analytically we find that

$$\begin{aligned}
&j\left(\frac{1}{2}(1+i\sqrt{39})\right) \\
&\quad = -\frac{27}{2}\left(6139474 + 1702799\sqrt{13} + 147\sqrt{39\left(89453213 + 24809858\sqrt{13}\right)}\right).
\end{aligned}$$

Note that as a corollary to this computation we can compute the following algebraic norm: $|j(\tau)| = 3^{15}17^3 23^3 29^3$. We could not have computed this from (1) alone since the discriminants -39 and -3 are not relatively prime.

4. Minimal polynomials of singular moduli from $\mathcal{X}_6^*$

For the Shimura curve $\mathcal{X}_6^*$, the idea is essentially the same. However, since there are no cusps on $\mathcal{X}_6^*$, there is no $\mathbf{q}$-expansion for the function $t : \mathcal{X}_6^* \to \mathbb{P}^1$. Hence the analog to (1) in the Shimura curve case is considerably more complicated to compute. In [19], Schofer uses Whittaker coefficients to attain an explicit formula for the average of a Borcherds form over CM points associated to a quadratic form of signature $(n, 2)$. In the second half of [20] Schofer shows that this generalizes the Gross-Zagier formula in the classical modular curve case. In [6] an explicit modular form whose Taylor coefficients play the role of the q-expansion is given and Schofer's techniques are then applied to the Shimura curves $\mathcal{X}_6^*$ and $\mathcal{X}_{10}^*$ to algebraically compute the norms of CM points on these curves. We now further extend these methods in a manner similar to the previous section to compute the minimal polynomials of the singular moduli on $\mathcal{X}_6^*$.

An area calculation [5] shows that $\mathcal{X}_6^*$ has genus 0 and so there exists a parameterization $t : \mathcal{X}_6^* \xrightarrow{\sim} \mathbb{P}^1$ over $\mathbb{Q}$. Such a map giving the isomorphism is only well defined up to a PGL_2 action on $\mathbb{P}^1$. However, the map is uniquely determined once the value at three points of $\mathcal{X}_6^*$ are chosen. Thus it suffices to assign its value at three CM points. Let s_d denote the CM point of discriminant d. In [5], Elkies shows that the triangle group Γ^* is generated by s_3, s_4 and s_{24} and makes the arbitrary, albeit natural, choice of defining the function's zeros and poles at those points. In [6], Errthum follows suit, defining a map such that

$$\begin{aligned} t(s_3) &= \infty, \\ t(s_4) &= 0, \\ t(s_{24}) &= 1. \end{aligned} \tag{2}$$

Then, using Schofer's techniques, he determines $|t(s_d)|$, the rational norm of the singular moduli of $\mathcal{X}_6^*$.

We can now construct the minimal polynomial for $t(s_d)$ much as we did for $j(\tau)$ in the previous section. In general, the algebraic degree of a singular modulus on a Shimura curve, $h(d)$, can be computed using genus theory [5]. For $\mathcal{X}_6^*$, there are exactly 27 rational singular moduli. Let ζ_d denote a rational singular moduli (e.g., ζ_d only makes sense for the 27 specific values of d for which the singular moduli is, in fact, rational). Then we can define a new parametrization t_d by making different choices than those in (2). Specifically, if we choose instead, for $d \neq 3, 4$,

$$\begin{aligned} t_d(s_3) &= \infty, \\ t_d(s_d) &= 0, \\ t_d(s_4) &= \zeta_d, \end{aligned} \tag{3}$$

it yields the relationship

$$t_d(x) = \zeta_d - t(x). \tag{4}$$

Note that although (3) alone does not uniquely define t_4, in light of (4) we can define $t_4 = -t$.

Again, for a given $s_{d'}$ we can compute $|t_d(s_{d'})|$ in two different ways—via the calculations in [6] and by definition:

$$\begin{aligned}
|t_d(s_{d'})| &= \left|\prod_\sigma \sigma(t_d(s_{d'}))\right| \\
&= \left|\prod_\sigma \sigma(\zeta_d - t(s_{d'}))\right| \\
&= \left|\prod_\sigma (\zeta_d - \sigma(t(s_{d'})))\right| \qquad \text{(since } \zeta_d \text{ is rational)} \\
&= |M_{t(s_{d'})}(\zeta_d)|.
\end{aligned}$$

Repeating this for $h(d')+1$ choices of r_d gives us sufficiently many points to exhaustively search the $2^{h(d')}$ possibilities for the monic polynomial $M_{t(s_{d'})}(x)$. Notice that since the calculations in [6] are not constrained by a property analogous to the relative primeness of discriminants, this method of calculation works for any singular modulus with $h(d') \le 26$. This yields a much larger collection of points than in the classical case.

4.1. **Example: $t_6(s_{244})$.** We now consider the case of the CM point $s_{244} \in \mathcal{X}_6^*$. Genus theory shows that the image of s_{244} is an algebraic number of degree 3. Since the norm calculator in the Shimura curve case does not require us to work with relatively prime discriminants, we can use the algorithms in [6] to compute the following:

$$\begin{aligned}
|t_4(s_{244})| &= \frac{2^6 3^{21} 19^4}{17^6 29^6}, \\
|t_{24}(s_{244})| &= \frac{19^4 37^2 47^2 61}{17^2 29^6}, \\
|t_{40}(s_{244})| &= \frac{3^{22} 83 \cdot 101 \cdot 107 \cdot 163}{5^9 17^2 29^4}, \\
|t_{52}(s_{244})| &= \frac{2^{18} 3^{23} 37^2 103 \cdot 131 \cdot 179 \cdot 199 \cdot 263}{5^{18} 17^6 29^6}.
\end{aligned}$$

This gives the following 4 points on the curve $y = |M_{t(s_{d'})}(x)|$:

$$\begin{aligned}
(x_1, y_1) &= \Big(0,\ \frac{2^6 3^{21} 19^4}{17^6 29^6}\Big), \\
(x_2, y_2) &= \Big(1,\ \frac{19^4 37^2 47^2 61}{17^2 29^6}\Big), \\
(x_3, y_3) &= \Big(-\frac{3^7}{5^3},\ \frac{3^{22} 83 \cdot 101 \cdot 107 \cdot 163}{5^9 17^2 29^4}\Big), \\
(x_4, y_4) &= \Big(\frac{2^2 3^7}{5^6},\ \frac{2^{18} 3^{23} 37^2 103 \cdot 131 \cdot 179 \cdot 199 \cdot 263}{5^{18} 17^6 29^6}\Big).
\end{aligned}$$

Using standard curve fitting, there are 8 different possibilities depending on the choices of sign for y_i. Only one choice of signs, namely

$$(x_1, -y_1),\ (x_2, y_2),\ (x_3, -y_3),\ (x_4, y_4),$$

yields a monic polynomial, which is

$$M_{t(s_{d'})}(x)=x^3-\frac{159511016412629892}{14357588953446649}x^2+\frac{2240284633411688496}{14357588953446649}x - \frac{87245036145162432}{14357588953446649}$$
$$=x^3-\frac{2^2 3^7 31\cdot 67\cdot 37223\cdot 235849}{17^6 29^6}x^2+\frac{2^4 3^{14} 151\cdot 1187\cdot 163327}{17^6 29^6}x-\frac{2^6 3^{21} 19^4}{17^6 29^6}.$$

This is only a degree 3 polynomial over the rationals and is thus solvable by radicals. As in the classical case, a floating point approximation of the CM point is required to determine which of the 3 roots it is. Although it is not easy to achieve an approximation by working complex analytically, Greenberg [9] has demonstrated an approach that uses the Cerednik-Drinfeld p-adic uniformization to compute a p-adic approximation.

5. Algebraic *abc*-ratios of singular moduli

Oesterle and Masser's well-known *abc*-conjecture states that for relatively prime positive integers that satisfy $a + b = c$ there is a bound on how large c can be in terms of the product of all the primes involved. More explicitly the conjecture asserts that given any $\epsilon > 0$ there is a constant C_ϵ such that

$$c \le C_\epsilon(\mathrm{rad}(abc))^{1+\epsilon}$$

where $\mathrm{rad}(n)$ is the product of all prime divisors of n.

Taking the constant as 1, one can measure the quality of an *abc*-example by the necessary size of ϵ. For this reason we consider the *abc*-ratio

$$\alpha(a,b,c) = \frac{\ln(c)}{\ln(\mathrm{rad}(abc))}.$$

To this date, the largest known *abc*-ratio is

$$\alpha(2, 3^{10}109, 23^5) \approx 1.62991.$$

For comparison, the median value of $\alpha(a,b,c)$ for $1 \le a, b \le 100$ is approximately 0.429 with the maximum being $\alpha(1, 80, 81) \approx 1.29203$. A standard threshold for the quality is 1.4 [4], [7], [14], so an *abc*-example with $\alpha(a,b,c) > 1.4$ is called good.

Vojta [21] generalized the *abc*-conjecture to number fields in the following way (as described in [14]). Let K be an algebraic number field and let V_K denote the set of primes on K. Then any $v \in V_K$ gives an equivalence class of nontrivial norms on K (finite or infinite). Let $||x||_v = |P|^{-v_P(x)}$ if v is a prime defined by a prime ideal P of the ring of integers O_K in K and v_P is the corresponding valuation, where $|\cdot|$ is the absolute norm. Let $||x||_v = |g(x)|^e$ for all nonconjugate embeddings $g : K \to \mathbb{C}$ with $e = 1$ if g is real and $e = 2$ if g is complex. Define the height of any triple a, b, $c \in K^\times$ to be

$$H_K(a,b,c) = \prod_{v\in V_K} \max(||a||_v, ||b||_v, ||c||_v),$$

and the radical (or conductor) of (a,b,c) by

$$\mathrm{rad}_K(a,b,c) = \prod_{P\in I_K(a,b,c)} |P|,$$

where $I_K(a,b,c)$ is the set of all prime ideals P of O_K for which $||a||_v$, $||b||_v$, $||c||_v$ are not equal. Let $D_{K/\mathbb{Q}}$ denote the discriminant of K.

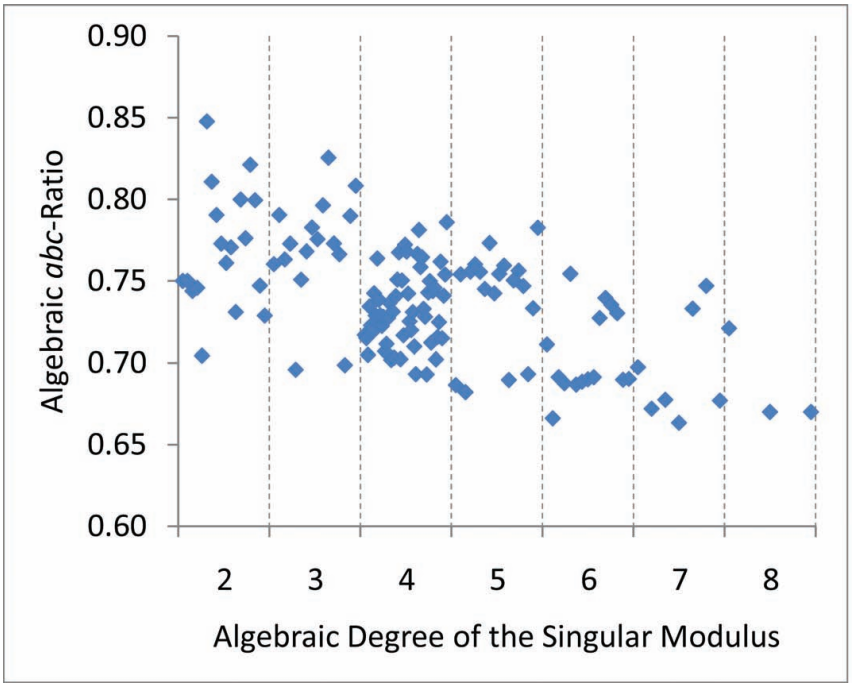

FIGURE 1. Algebraic *abc*-ratio for classical singular moduli

The (uniform) algebraic *abc*-conjecture then states that for any $\epsilon > 0$, there exists a positive constant C_ϵ such that for all a, b, $c \in K^\times$ satisfying $a+b+c=0$, we have

$$H_K(a,b,c) < C_\epsilon^{[K:\mathbb{Q}]}(|D_{K/\mathbb{Q}}|\mathrm{rad}_K(a,b,c))^{1+\epsilon}.$$

Again, constraining the constant leads to a measure of the quality of an algebraic *abc*-example given by the algebraic *abc*-ratio

$$\gamma(a,b,c) = \frac{\ln(H_K(a,b,c))}{\ln(D_{K/\mathbb{Q}}) + \ln(\mathrm{rad}_K(a,b,c))}.$$

The largest known algebraic *abc*-ratio is

$$\gamma(w,(w+1)^{10}(w-1),2^9(w+1)^5) \approx 2.029229$$

where $w^2 - w - 3 = 0$. Since algebraic *abc*-ratios are in general slightly larger than *abc*-ratios, any example with $\gamma(a,b,c) > 1.5$ is considered good [2], [14].

In [8] the authors suggest that there might exist a large number of good *abc*-examples in the collection of singular moduli. For instance, (1) indicates that the norms of singular moduli are small primes to large powers. In [5] the *abc*-ratios of the rational singular moduli on $\mathcal{X}_6^*$ are computed, noting that none of them are close to being good. In fact, most of the rational singular moduli on $\mathcal{X}_6^*$ have an *abc*-ratio less than 1. Since the algebraic *abc*-ratio is Galois-invariant, it is sufficient to know only the minimal polynomial for the algebraic number involved. Thus, with the minimal polynomial available for singular moduli of the classical modular curve and the Shimura curve $\mathcal{X}_6^*$, we can continue this search by computing their algebraic *abc*-ratios. Figure 1 presents a plot of $\gamma(a,b,c)$ versus $[K:\mathbb{Q}]$ for the

classical singular moduli. Figure 2 does the same for the Shimura curve $\mathcal{X}_6^*$. (Note: Data points with common degree were lexicographically ordered according to the coefficients of the minimal polynomial. Not all data points were available for the classical singular moduli due to software reaching computational limits. For $\mathcal{X}_6^*$, all data points of singular moduli up to the discriminant of 4744 are plotted.)

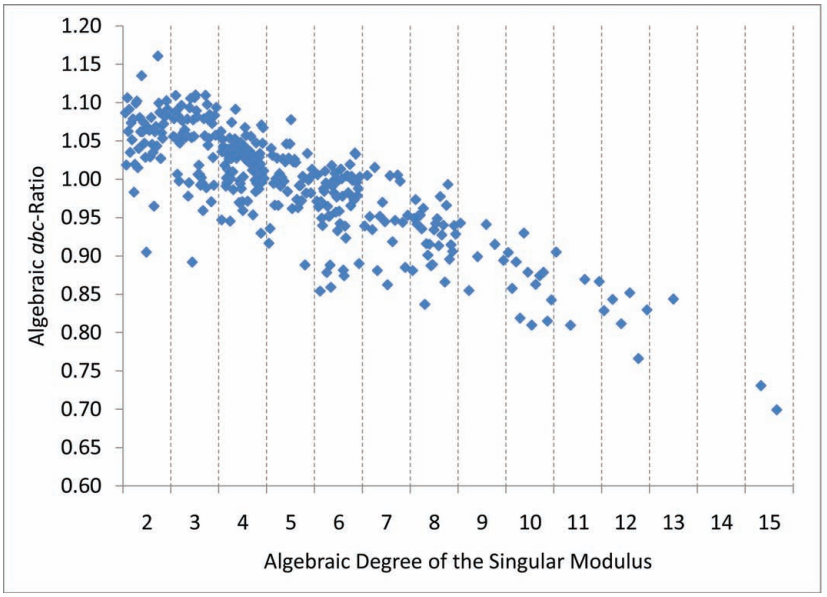

FIGURE 2. Algebraic *abc*-ratio for $\mathcal{X}_6^*$ singular moduli

Similar to [5], in neither case are any good *abc*-examples found. Furthermore, the *abc*-ratios appear to be following a decreasing trend as the degree increases, putting doubt on the likelihood of finding good high-degree examples in singular moduli. In fact, it may be possible to use the general formulas in [19] to construct lower and upper bounds on the algebraic *abc*-ratios of singular moduli.

6. Extensions and Limitations

As noted in Section 3, there is a definite cut-off in the degree of the minimal polynomials that are able to be calculated. This cut-off is dictated by the number of rational CM points on the classical modular curve and is a by-product of the Gross-Zagier formula's limitation to only compute rational norms. If one had a method of computing the norm down to any extension $F/\mathbb{Q}$ of $j(\tau_1) - j(\tau_2)$, then the methods in this paper could be salvaged in the following way. Fix a CM point τ of class number h and find the smallest extension field F such that $j(\tau_i) \in F$ for at least $h+1$ CM points. Then the minimal polynomial for τ could be interpolated over F. For example, in the classical case there are six additional singular moduli in $\mathbb{Q}(\sqrt{5})$. Knowing a Gross-Zagier formula for this field would allow the methods of this paper to extend to finding the minimal polynomials over $\mathbb{Q}(\sqrt{5})$ of singular moduli of degree 14 or less. Likewise, extending the generalization of Gross-Zagier given by Schofer to extension fields would allow the methods shown here to apply to higher degree singular moduli of Shimura curves.

References

1. Baier, H., *Efficient Computation of Singular Moduli with Application in Cryptography.* Fundamentals of Computation Theory (Riga, 2001), 71–82, Lecture Notes in Comput. Sci., **2138**, Springer, Berlin, 2001. MR1914098 (2003e:94062)
2. Broberg, N., *Some examples related to the abc-conjecture for algebraic number fields*, Math. Comput. **69** (232) (2000) 1707–1710. MR1659863 (2001a:11177)
3. Cox, D.A., *Primes of the Form $x^2 + ny^2$.* John Wiley & Sons, 1989. MR1028322 (90m:11016)
4. Dokchitser, T., *LLL & ABC*, J. Number Theory **107**, No. 1, 161–167 (2004). MR2059955 (2005d:11040)
5. Elkies, N., *Shimura curve computations.* Algorithmic Number Theory (Portland, Oregon, 1998), 1-47, Lecture Notes in Comput. Sci., **1423**, Springer, Berlin, 1998. MR1726059 (2001a:11099)
6. Errthum, E., *Singular Moduli of Shimura Curves.* Canadian Journal of Mathematics **63** (2011), 826–861. doi:10.4153/CJM-2011-023-7. MR2848999
7. Geuze, G. and de Smit, B. *Reken mee met ABC.* Nieuw Archief voor Wiskunde (5th series) 8 (2007), 26-30 MR2340133
8. A. Granville and H. M. Stark, *ABC implies no Siegel zeros for L-functions of characters with negative discriminant.* Invent. Math. **139** (2000), 509–523. MR1738058 (2002b:11114)
9. Greenberg, M. *Computing Heegner points arising from Shimura curve parametrizations.* Arithmetic Geometry, 115–124, Clay Math. Proc., 8, Amer. Math. Soc., Providence, RI, 2009. MR2498058 (2010h:11091)
10. Gross, B. and Zagier, D., *On singular moduli*, J. Reine Angew. Math. **355** (1985), 191-220. MR772491 (86j:11041)
11. Katok, S. *Fuchsian groups*, University of Chicago Press, Chicago, 1992. MR1177168 (93d:20088)
12. *Magma Calculator*, http://magma.maths.usyd.edu.au/calc/, 2010
13. Masser, D. W. *Note on a conjecture of Szpiro.* Séminaire sur les Pinceaux de Courbes Elliptiques (Paris, 1988). Astérisque **183** (1990), 19–23. MR1065152 (91g:11058)
14. Nitaj, A. *The ABC Conjecture Homepage*, http://www.math.unicaen.fr/ nitaj/abc.html, May 27, 2010.
15. Oesterlé, J., *Nouvelles approches du "théorème" de Fermat*, Séminaire Bourbaki no. 694 (1987-1988), Astérisque **161-162** (1988), 165-186. MR992208 (90g:11038)
16. Ono, K., *The web of modularity: arithmetic of the coefficients of modular forms and q-series*, Published for the Conference Board of the Mathematical Sciences, Washington, DC, 2004. MR2020489 (2005c:11053)
17. Roberts, D. P., *Shimura curves analagous to $X_0(N)$*. Ph.D. Thesis, Harvard University, 1989. MR2637583
18. Shimura, G., *Introduction to the arithmetic theory of automorphic functions*, Math. Soc. Japan (1971). MR0314766 (47:3318)
19. Schofer, J. *Borcherds forms and generalizations of singular moduli*, J. Reine Angew. Math. **629** (2009), 1-36. MR2527412 (2011a:11095)
20. Schofer, J. *Borcherds forms and generalizations of singular moduli*, Ph.D. Thesis, University of Maryland, College Park, 2005. MR2707427
21. Vojta, P., *Diophantine Approximations and Value Distribution Theory*, Lecture Notes in Math. **1239**. Springer-Verlag, Berlin and New York, 1987. MR883451 (91k:11049)

Department of Mathematics and Statistics, Winona State University, Winona, Minnesota 55987

E-mail address: eerrthum@winona.edu