MATHEMATICS OF COMPUTATION
Volume 85, Number 301, September 2016, Pages 2499–2514
http://dx.doi.org/10.1090/mcom3057
Article electronically published on December 9, 2015

COMPUTING THE MAZUR AND SWINNERTON-DYER CRITICAL SUBGROUP OF ELLIPTIC CURVES

HAO CHEN

Abstract. Let E be an optimal elliptic curve defined over $\mathbb{Q}$. The *critical subgroup* of E is defined by Mazur and Swinnerton-Dyer as the subgroup of $E(\mathbb{Q})$ generated by traces of branch points under a modular parametrization of E. We prove that for all rank two elliptic curves with conductor smaller than 1000, the critical subgroup is torsion. First, we define a family of *critical polynomials* attached to E and develop two algorithms to compute such polynomials. We then give a sufficient condition for the critical subgroup to be torsion in terms of the factorization of critical polynomials. Finally, a table of critical polynomials is obtained for all elliptic curves of rank two and conductor smaller than 1000, from which we deduce our result.

1. Introduction

1.1. **Preliminaries.** Let E be an elliptic curve over $\mathbb{Q}$ and let $L(E,s)$ be the L-function of E. The rank part of the Birch and Swinnerton-Dyer (BSD) conjecture states that

$$\operatorname{rank}(E(\mathbb{Q})) = \operatorname{ord}_{s=1} L(E,s).$$

The right hand side is called the *analytic rank of* E and is denoted by $r_{\mathrm{an}}(E)$. The left hand side is called the *algebraic rank of* E. The rank part of the BSD conjecture is still open when $r_{\mathrm{an}}(E) > 1$, and its proof for the case $r_{\mathrm{an}}(E) = 1$ uses the *Gross-Zagier formula*, which relates the value of certain L-functions to heights of Heegner points.

Let N denote the conductor of E. The modular curve $X_0(N)$ is a nonsingular projective curve defined over $\mathbb{Q}$. Since E is modular (Breuil, Conrad, Diamond, and Taylor [BCDT01]), there is a surjective morphism $\varphi : X_0(N) \to E$ defined over $\mathbb{Q}$. Let ω_E be the invariant differential on E and let $\omega = \varphi^*(\omega_E)$. Then ω is a holomorphic differential on $X_0(N)$, and we have $\omega = cf(z)dz$, where f is the normalized newform attached to E and c is a nonzero constant. In the rest of the paper, we fix the following notation: the elliptic curve E, the conductor N, the morphism φ, and the differential ω. Let R_φ denote the ramification divisor of φ.

Definition 1.1 (Mazur and Swinnerton-Dyer [MSD74])**.** The *critical subgroup* of E is

$$E_{\mathrm{crit}}(\mathbb{Q}) = \langle \operatorname{tr}(\varphi([z])) : [z] \in \operatorname{supp} R_\varphi \rangle,$$

where $\operatorname{tr}(P) = \sum_{\sigma:\mathbb{Q}(P)\to\bar{\mathbb{Q}}} P^\sigma$.

Received by the editor January 17, 2015 and, in revised form, March 1, 2015 and March 18, 2015.

2010 *Mathematics Subject Classification.* Primary 11G05.

©2015 Hao Chen

Since the divisor R_φ is defined over $\mathbb{Q}$, every point $[z]$ in its support is in $X_0(N)(\overline{\mathbb{Q}})$, hence $\varphi([z]) \in E(\overline{\mathbb{Q}})$, justifying the trace operation. The group $E_{\mathrm{crit}}(\mathbb{Q})$ is a subgroup of $E(\mathbb{Q})$. Observe that $R_\varphi = \mathrm{div}(\omega)$; thus $\deg R_\varphi = 2g(X_0(N)) - 2$. In the rest of the paper, we use the notation $\mathrm{div}(\omega)$ in place of the ramification divisor R_φ. In addition, we will assume E is an optimal elliptic curve, so φ is unique up to sign. This justifies the absence of φ in the notation $E_{\mathrm{crit}}(\mathbb{Q})$.

Recall the construction of *Heegner points*: for an imaginary quadratic order $\mathcal{O} = \mathcal{O}_d$ of discriminant $d < 0$, let $H_d(x)$ denote its *Hilbert class polynomial*.

Definition 1.2. A point $[z] \in X_0(N)$ is a *generalized Heegner point* if there exists a negative discriminant d s.t. $H_d(j(z)) = H_d(j(Nz)) = 0$. If in addition we have $(d, 2N) = 1$, then $[z]$ is a *Heegner point*.

For any discriminant d, let E_d denote the quadratic twist of E by d. Then the Gross-Zagier formula in [GZ86] together with a non-vanishing theorem for $L(E_d, 1)$ (see, for example, Bump, Friedberg, and Hoffstein [BFH90]) implies the following.

Theorem 1.3.
(1) If $r_{\mathrm{an}}(E) = 1$, then there exists a Heegner point $[z]$ on $X_0(N)$ such that $\mathrm{tr}(\varphi([z]))$ has infinite order in $E(\mathbb{Q})$.
(2) If $r_{\mathrm{an}}(E) \geq 2$, then $\mathrm{tr}(\varphi([z])) \in E(\mathbb{Q})_{\mathrm{tors}}$ for every "generalized Heegner point" $[z]$ on $X_0(N)$.

The first case in the above theorem is essential to the proof of the rank BSD conjecture for $r_{\mathrm{an}}(E) = 1$. We observe that the defining generators of the critical subgroup also take the form $\mathrm{tr}(\varphi([z]))$. Then a natural question is:

Question 1.4. Does there exist an elliptic curve E defined over $\mathbb{Q}$ such that $r_{\mathrm{an}}(E) \geq 2$ and $\mathrm{rank}(E_{\mathrm{crit}}(\mathbb{Q})) > 0$?

We will show that the answer is negative for all elliptic curves with conductor $N < 1000$, using *critical polynomials* attached to elliptic curves.

1.2. **Main results.** Let E, N, φ, and ω be as defined previously, and write $\mathrm{div}(\omega) = \sum_{[z] \in X_0(N)} n_z [z]$. Let j denote the j-invariant function.

Definition 1.5. The *critical j-polynomial* of E is

$$F_{E,j}(x) = \prod_{z \in \mathrm{supp}\, \mathrm{div}(\omega), j(z) \neq \infty} (x - j(z))^{n_z}.$$

Because $\mathrm{div}(\omega)$ is defined over $\mathbb{Q}$ and has degree $2g(X_0(N))-2$, we have $F_{E,j}(x) \in \mathbb{Q}[x]$ and $\deg F_{E,j} \leq 2g(X_0(N)) - 2$, where equality holds if $\mathrm{div}(\omega)$ does not contain cusps. For any nonconstant modular function $h \in \mathbb{Q}(X_0(N))$, the *critical h-polynomial* of E is defined similarly by replacing j with h.

In this paper we give two algorithms, *Poly Relation* and *Poly Relation-YP*, to compute critical polynomials. The algorithm *Poly Relation* computes the critical j-polynomial $F_{E,j}$, and the algorithm *Poly Relation-YP* computes the critical h-polynomial $F_{E,h}$ for some modular function h chosen within the algorithm. We then relate the critical polynomials to the critical subgroup via the following theorem.

Theorem 1.6. *Suppose $r_{\mathrm{an}}(E) \geq 2$, and assume at least one of the following holds:*

(1) $F_{E,h}$ is irreducible for some nonconstant function $h \in \mathbb{Q}(X_0(N))$.

(2) There exist negative discriminants D_k and positive integers s_k for $1 \leq k \leq m$ with $\mathbb{Q}(\sqrt{D_k}) \neq \mathbb{Q}(\sqrt{D_{k'}})$ for all $k \neq k'$ and an irreducible polynomial $F_0 \in \mathbb{Q}[x]$, such that

$$F_{E,j} = \prod_{k=1}^{m} H_{D_k}^{s_k} \cdot F_0.$$

Then $\mathrm{rank}(E_{\mathrm{crit}}(\mathbb{Q})) = 0$.

Combining Theorem 1.6 with our computation of critical polynomials, we verify the main result of this paper stated in the following corollary.

Corollary 1.7. *For all elliptic curves E of analytic rank two and conductor smaller than* 1000*, the rank of $E_{\mathrm{crit}}(\mathbb{Q})$ is zero.*

This paper is organized as follows: in Sections 2 and 3, we describe the algorithms *Poly Relation* and *Poly Relation-YP*. In Section 4, we prove Theorem 1.6. Lastly, in Section 5, we show a table of critical polynomials for all elliptic curves with rank two and conductor smaller than 1000 and prove Corollary 1.7.

2. The algorithm *Poly Relation*

Let $C/\mathbb{Q}$ be a nonsingular projective curve. For a rational function $r \in \mathbb{Q}(C)$, let $\mathrm{div}_0(r)$ and $\mathrm{div}_\infty(r)$ denote its divisor of zeros and poles, respectively, and define $\deg r = \deg(\mathrm{div}_0(r))$.

Definition 2.1. Let $C/\mathbb{Q}$ be a nonsingular projective curve, and let r, u be two nonconstant rational functions on C. A *minimal polynomial relation between r and u* is an irreducible polynomial $P(x,y) \in \mathbb{Q}[x,y]$ such that $P(r,u) = 0$, $\deg_x(P) \leq \deg u$ and $\deg_y(P) \leq \deg r$.

A minimal polynomial relation always exists and is unique up to scalar multiplication. Write $\mathrm{div}(r) = \sum_{[z] \in X_0(N)} n_z[z]$ and $P(x,y) = f_n(y)x^n + \cdots + f_1(y)x + f_0(y)$.

Proposition 2.2. *If $\mathbb{Q}(C) = \mathbb{Q}(r,u)$ and $\gcd(f_0(y), f_n(y)) = 1$, then there is a constant $c \neq 0$ s.t.*

$$f_0(y) = c \prod_{z \in \mathrm{div}_0(r) \setminus \mathrm{div}_\infty(u)} (y - u(z))^{n_z}.$$

Proof. Dividing $P(x,y)$ by $f_n(y)$ and replacing y by u, we get $x^n + \cdots + \frac{f_0(u)}{f_n(u)}$, which is a minimal polynomial of r over $\mathbb{Q}(u)$. So $\mathrm{Norm}_{\mathbb{Q}(r,u)/\mathbb{Q}(u)}(r) = \frac{f_0(u)}{f_n(u)}$. The rest of the proof uses a fact on extensions of valuations (see, for example, [Ste, Theorem 17.2.2]), which we now quote.

Lemma 2.3. *Suppose v is a nontrivial valuation on a field K and let L be a finite extension of K. Then for any $a \in L$,*

$$\sum_{1 \leq j \leq J} w_j(a) = v(\mathrm{Norm}_{L/K}(a)),$$

where the w_j are normalized valuations equivalent to extensions of v to L.

We continue with the proof. For any $z_0 \in C$ such that $u(z_0) \neq \infty$, consider the valuation $v = \mathrm{ord}_{(u-u(z_0))}$ on $\mathbb{Q}(u)$. The set of extensions of v to $\mathbb{Q}(C) = \mathbb{Q}(r,u)$ is in bijection with $\{z \in C : u(z) = u(z_0)\}$. Take $a = r$ and apply Lemma 2.3; we obtain

$$\sum_{z:u(z)=u(z_0)} \mathrm{ord}_z(r) = \mathrm{ord}_{u-u(z_0)} \frac{f_0(u)}{f_n(u)}.$$

Combining the identities for all $z_0 \in C \setminus \mathrm{div}_\infty(u)$, we have for some constant c,

$$\prod_{z\in \mathrm{div}(r):u(z)\neq\infty} (y-u(z))^{n_z} = c \cdot \frac{f_0(y)}{f_n(y)}.$$

If $r(z) = 0$, then the condition $\gcd(f_0(y), f_n(y)) = 1$ implies that $f_0(u(z)) = 0$ and $f_n(u(z)) \neq 0$. Therefore, since $\gcd(f_0, f_n) = 1$, we must have

$$f_0(y) = c \prod_{z\in \mathrm{div}_0(r)\setminus \mathrm{div}_\infty(u)} (y-u(z))^{n_z}.$$

This completes the proof. □

For later use, we also deal with the case where $u(z) = \infty$, which was left out in the above proof. The corresponding valuation on $\mathbb{Q}(u)$ is ord_∞, defined by $\mathrm{ord}_\infty(g/h) = \deg g - \deg h$ for $0 \neq g, h \in \mathbb{Q}[u]$. We derive that

$$\sum_{z:u(z)=\infty} \mathrm{ord}_z(r) = \deg f_n - \deg f_0.$$

Next we apply Proposition 2.2 to the computation of $F_{E,j}$. In the rest of the paper, $\mathrm{d}j = j'(z)dz$ is viewed as a differential on $X_0(N)$. Fix the following two modular functions on $X_0(N)$:

$$r = j(j-1728)\frac{\omega}{\mathrm{d}j},\ u = \frac{1}{j}. \tag{2.1}$$

First we compute the divisor of r. Let $\mathcal{E}_2(N)$ and $\mathcal{E}_3(N)$ denote the set of elliptic points of period 2 and 3 on $X_0(N)$, respectively. Then

(2.2)

$$\mathrm{div}(\mathrm{d}j) = -j^*(\infty) - \sum_{c=cusp} c + \frac{1}{2}\left(j^*(1728) - \sum_{z\in\mathcal{E}_2(N)} z\right) + \frac{2}{3}\left(j^*(0) - \sum_{z\in\mathcal{E}_3(N)} z\right).$$

Writing $j^*(\infty) = \sum_{c=cusp} e_c[c]$, we obtain

$$\begin{aligned}\mathrm{div}(r) = \mathrm{div}(\omega) &+ \frac{1}{2}\left(j^*(1728) + \sum_{z\in\mathcal{E}_2(N)} z\right) + \frac{1}{3}\left(j^*(0) + 2\sum_{z\in\mathcal{E}_3(N)} z\right) \\ &- \sum_{c=cusp} (e_c - 1)[c].\end{aligned} \tag{2.3}$$

Note that (2.3) may not be the simplified form of $\mathrm{div}(r)$, due to possible cancellations when $\mathrm{supp}\,\mathrm{div}(\omega)$ contains cusps. But since the definition of $F_{E,j}$ only involves critical points that are not cusps, the form of $\mathrm{div}(r)$ in (2.3) works fine for our purpose.

Next we show $\mathbb{Q}(r,u) = \mathbb{Q}(X_0(N))$ for the functions r, u in (2.1). For $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and a modular form f of weight two on some congruence subgroup,

we use $f|[\alpha]$ to denote the function $f|[\alpha](z) = (cz+d)^{-2} f(\frac{az+b}{cz+d})$. First we prove a lemma.

Lemma 2.4. *Let $N > 1$ be an integer and $f \in S_2(\Gamma_0(N))$ a normalized newform. Suppose $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ and $f|[\alpha] = f$; then $\alpha \in \Gamma_0(N)$.*

Proof. Write $\alpha = \left(\begin{smallmatrix} a & b \\ M & d \end{smallmatrix}\right)$. First we show that it suffices to consider the case where $d = 1$. Since $\gcd(M, d) = 1$, there exist $y, w \in \mathbb{Z}$ such that $My + dw = 1$. By replacing (y, w) with $(y + kd, w - kM)$ if necessary, we may assume $\gcd(y, N) = 1$. Now we can find $x, z \in \mathbb{Z}$ such that $\gamma = \left(\begin{smallmatrix} x & y \\ Nz & w \end{smallmatrix}\right) \in \Gamma_0(N)$ satisfies $\alpha\gamma = \left(\begin{smallmatrix} * & * \\ M & 1 \end{smallmatrix}\right)$. Note that $f|[\alpha\gamma] = f|[\gamma] = f$. We then further reduce to the case where $\alpha = \left(\begin{smallmatrix} 1 & 0 \\ M & 1 \end{smallmatrix}\right)$ by noticing that $\left(\begin{smallmatrix} 1 & -b \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma_0(N)$ and

$$\left(\begin{smallmatrix} 1 & -b \\ 0 & 1 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} a & b \\ M & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ M & 1 \end{smallmatrix}\right).$$

Let $w_N = \left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)$ be the matrix of the Fricke involution on $X_0(N)$. Then $f|[w_N] = \pm f$; hence $f|[w_N \alpha w_N] = f$. Since $w_N \alpha w_N = \left(\begin{smallmatrix} -N & M \\ 0 & -N \end{smallmatrix}\right)$, we have $f(q) = f|[\left(\begin{smallmatrix} -N & M \\ 0 & -N \end{smallmatrix}\right)](q) = f(q\zeta_N^{-M})$, where $\zeta_N = e^{\frac{2\pi i}{N}}$. The leading term of $f(q)$ is q, while the leading term of $f(q\zeta_N^{-M})$ is $\zeta_N^{-M} q$. So we must have $\zeta_N^{-M} = 1$, i.e., $N \mid M$. Hence $\alpha \in \Gamma_0(N)$ and the proof is complete. □

Proposition 2.5. *Let r, u be the two functions on $X_0(N)$ defined in* (2.1)*; then $\mathbb{Q}(r, u) = \mathbb{Q}(X_0(N))$.*

Proof. Consider the modular curve $X(N)$ defined over the field $K = \mathbb{Q}(\mu_N)$. Its function field $K(X(N))$ is a Galois extension of $K(u)$ containing $K(X_0(N))$. It follows that the conjugates of r in the extension $K(X(N))/K(u)$ are of the form $r_i = r|[\alpha_i]$ where $\{\alpha_i\}$ is a set of coset representatives of $\Gamma_0(N)\backslash \mathrm{SL}_2(\mathbb{Z})$. Note that $\mathbb{Q}(r, u) = \mathbb{Q}(X_0(N))$ if and only if the r_i are distinct. Suppose towards contradiction that there exists $i \neq k$ such that $r|[\alpha_i] = r|[\alpha_k]$. Since the function j and its derivative j' are invariant under the action of $\mathrm{SL}_2(\mathbb{Z})$, we see that $f|[\alpha_i] = f|[\alpha_k]$. Let $\alpha = \alpha_i \alpha_k^{-1}$; then $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ and $f|[\alpha] = f$. Now Lemma 2.4 implies $\alpha \in \Gamma_0(N)$, from which we derive $\Gamma_0(N)\alpha_i = \Gamma_0(N)\alpha_k$, a contradiction. □

Lemma 2.6. *Let g be the genus of $X_0(N)$. If $T \geq 2g-2$ is a positive integer, then rj^T and u satisfy the second condition of Proposition* 2.2*.*

Proof. Let $r_1 = rj^T$. When $T \geq 2g - 2$, the support of $\mathrm{div}_\infty(r_1)$ is the set of all cusps. Suppose $\gcd(f_n, f_0) > 1$. Let $p(y)$ be an irreducible factor of $\gcd(f_0, f_n)$. We keep the notation $K = \mathbb{Q}(\zeta_N)$ and consider the valuation ord_p on the field $K(y)$. Since $P(x, y)$ is irreducible, there exists an integer i with $0 < i < n$ such that $p(y) \nmid f_i$. Thus the Newton polygon of P with respect to the valuation ord_p has at least one edge with negative slope and one edge with positive slope. Therefore, for any Galois extension of L of $K(u)$ containing $K(r, u)$ and any valuation $\mathrm{ord}_\mathfrak{p}$ on L extending ord_p, where $\mathfrak{p}$ is an irreducible polynomial in $L[y]$ dividing $p(y)$, there exist two conjugates r', r'' of r_1 such that $\mathrm{ord}_\mathfrak{p}(r') < 0$ and $\mathrm{ord}_\mathfrak{p}(r'') > 0$. Take $L = K(X(N))$, then $\mathrm{div}_0(r') \cap \mathrm{div}_\infty(r'') \neq \emptyset$. But all conjugates of r_1 in $K(X(N))/K(u)$ are of the form $r_1(\alpha z)$ for some $\alpha \in \mathrm{SL}_2(\mathbb{Z})$. Hence the set of poles of any conjugate of r_1 is the set of all cusps on $X(N)$, a contradiction. □

Note that for any integer T, we have $\mathbb{Q}(rj^T, u) = \mathbb{Q}(r, u) = \mathbb{Q}(X_0(N))$. Hence when $T \geq 2g-2$, the pair (rj^T, u) satisfies both assumptions of Proposition 2.2. We thus obtain

Theorem 2.7. *Let $T \geq 2g-2$ be a positive integer and let*

$$P(x,y) = f_n(y)x^n + \cdots + f_1(y)x + f_0(y)$$

be a minimal polynomial relation of rj^T and u. Then there exist integers A, B and a nonzero constant c such that

$$F_{E,j}(y) = cf_0(1/y) \cdot y^A (y-1728)^B.$$

The integers A and B are defined as follows. For $i = 2$ or 3, let $\epsilon_i(N) = |\mathcal{E}_i(N)|$ denote the number of elliptic points on $X_0(N)$ of period i, and let d_N denote the index $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)]$. Then $A = \deg f_n - T \cdot d_N - \frac{1}{3}(d_N + 2\epsilon_3(N))$ and $B = -\frac{1}{2}(d_N + \epsilon_2(N))$.

Proof. Write $\mathrm{div}(\omega) = \sum_{[z] \in X_0(N)} n_z[z]$. Applying Proposition 2.2 to rj^T and u, we get

$$\text{(a)} \qquad \prod_{z:u(z)\neq 0,\infty} (y-u(z))^{n_z} \cdot (y-1/1728)^{\frac{1}{2}(d_N+\epsilon_2(N))} = cf_0(y)$$

and

$$\text{(b)} \qquad \sum_{z:u(z)=\infty} \mathrm{ord}_z(\omega) + T \cdot d_N + \frac{1}{3}(d_N + 2\epsilon_3(N)) = \deg f_n - \deg f_0.$$

To change from $u = \frac{1}{j}$ to j, we replace y by $1/y$ in (a) and multiply both sides by $y^{\deg f_0}$ to obtain

$$\prod_{z:j(z)\neq 0,\infty} (y-j(z))^{n_z} \cdot (y-1728)^{\frac{1}{2}(d_N+\epsilon_2(N))} = cf_0(1/y)y^{\deg f_0}.$$

The contribution of $\{z \in \mathrm{div}(\omega) : j(z) = 0\}$ to $F_{E,j}$ can be computed using (b), so

$$\begin{aligned} F_{E,j}(y) &= c \cdot y^{\deg f_n - \deg f_0 - T\cdot d_N - \frac{1}{3}(d_N+2\epsilon_3(N))} y^{\deg f_0} \\ &\quad \cdot (y-1728)^{-\frac{1}{2}(d_N+\epsilon_2(N))} f_0(1/y) \\ &= c \cdot y^{\deg f_n - T\cdot d_N - \frac{1}{3}(d_N+2\epsilon_3(N))} (y-1728)^{-\frac{1}{2}(d_N+\epsilon_2(N))} f_0(1/y). \end{aligned}$$

□

Now we describe the algorithm *Poly Relation*.

Algorithm 1 *Poly Relation*

Input: E = elliptic curve over $\mathbb{Q}$; N = conductor of E; f = the newform attached to E; $g = g(X_0(N))$, d_N, $\epsilon_2(N)$, $\epsilon_3(N)$, and c_N = number of cusps of $X_0(N)$.
Output: The critical j-polynomial $F_{E,j}(x)$.

1: Fix a sufficiently large integer M. $T := 2g-2$.
2: $r := j^{2g-1}(j-1728)\frac{f}{j'}$, $u := \frac{1}{j}$.
3: $\deg r := (2g-1)d_N - c_N$, $\deg u := d_N$.
4: Compute the q-expansions of r and u to q^M.
5: Let $\{c_{a,b}\}_{0\le a\le \deg u, 0\le b\le \deg r}$ be unknowns; compute a vector that spans the one-dimensional vector space
$K = \{(c_{a,b}) : \sum c_{a,b} r(q)^a u(q)^b \equiv 0 \pmod{q^M}\}$.
6: $P(x,y) := \sum c_{a,b} x^a y^b$. Write $P(x,y) = f_n(y)x^n + \cdots + f_1(y)x + f_0(y)$.
7: $A := \deg f_n - T\cdot d_N - \frac{1}{3}(d_N + 2\epsilon_3(N))$, $B := -\frac{1}{2}(d_N + \epsilon_2(N))$.
8: Output $F_{E,j}(x) = cf_0(1/x)\cdot x^A (x-1728)^B$.

Note that in the above algorithm, the integer M can be taken to be $2\deg r \deg u + 1$ by the following lemma.

Lemma 2.8. *Let $r, u \in \mathbb{Q}(X_0(N))$ be nonconstant functions. If there is a polynomial $P \in \mathbb{Q}[x,y]$ such that $\deg_x P \le \deg u$, $\deg_y P \le \deg r$, and*

$$P(r,u) \equiv 0 \pmod{q^M}$$

for some $M > 2\deg u \deg r$, then $P(r,u) = 0$.

Proof. Suppose $P(r,u)$ is nonconstant as a rational function on $X_0(N)$. Then $\deg P(r,u) \le \deg(r^{\deg u} u^{\deg r}) = 2\deg u \deg r$. It follows from $P(r,u) \equiv 0 \pmod{q^M}$ that $\operatorname{ord}_{[\infty]} P(r,u) \ge M$. Since $M > 2\deg u \deg r$, the number of zeros of $P(r,u)$ is greater than its number of poles, a contradiction. Thus $P(r,u)$ is a constant function. But then $P(r,u)$ must be 0 since it has a zero at $[\infty]$. This completes the proof. □

Remark 2.9. When N is square free, there is a faster method that computes $F_{E,j}$ by computing the *Norm* of the modular form f, defined as $\operatorname{Norm}(f) = \prod f|[A_i]$, where $\{A_i\}$ is a set of right coset representatives of $\Gamma_0(N)$ in $\mathrm{SL}_2(\mathbb{Z})$. This approach is inspired by Ahlgren and Ono [AO03], where the authors presented an algorithm to compute the j-polynomials of Weierstrass points on $X_0(p)$ when p is prime.

Remark 2.10. In practice, in order to make the algorithm faster, we make different choices of r to make $\deg r$ small. Let η denote the Dedekind η-function and let $\Delta = \eta^{24}$ denote the discriminant modular form of level 1 and weight 12. Suppose $4 \mid N$, and let $r_4 = \frac{\omega j h_2}{\mathrm{d}j(32+h_4)}$, where $h_2 = \frac{\Delta(z)-512\Delta(2z)}{\Delta(z)+256\Delta(2z)}$ and $h_4 = (\eta(z)/\eta(4z))^8$. Then $\operatorname{div}(r_4) = \operatorname{div}(\omega) + D - D'$, where D and D' are supported on the cusps of $X_0(N)$, and $\deg D = c_N - \delta$, where δ is the number of cusps on $X_0(N)$ whose images in $X_0(4)$ are equivalent to $[\infty]$. Hence r_4 has a relatively small degree and is better suited for computation.

Remark 2.11. In order to speed up the computation, instead of taking $T = 2g-2$ in the algorithm, we may take $T = 0$. First, if $\operatorname{div}(\omega)$ does not contain cusps (for example, this happens if N is square free), then the functions r and u already satisfy the assumptions of Proposition 2.2. Second, if $\operatorname{div}(\omega)$ does contain cusps,

then $\deg(r)$ will be smaller than its set value in the algorithm due to cancellation between zeros and poles. As a result, the vector space K will have dimension greater than 1. Nonetheless, using a basis of K, we could construct a set of polynomials $P_i(x,y)$ with $P_i(r,u) = 0$. Now $P(x,y)$ is the greatest common divisor of the $P_i(x,y)$.

We discuss the complexity of the algorithm *Poly Relation*. The complexity of step 5 is dominant, where the kernel of a linear map is computed. Let C denote the matrix of the linear map. We use the algorithm of Mulders and Storjohann [MS04] for the kernel computation, which has time complexity $O(nmr \log ||C||)^{1+o(1)}$, where n, m are the number of rows and columns of C, r is the rank of C, and $||C|| = \max\{|C_{ij}|\}$.

In our case, let $d_N = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)]$. Then the number of rows and columns of C are bounded by $2d_N^2$ and d_N^2, respectively. The rank of C is equal to the number of columns minus one, hence is bounded by d_N^2. The entries in C are the coefficients of polynomials in q of form $r(q)^a u(q)^b \pmod M$, where $0 \le a \le \deg u$ and $0 \le b \le \deg r$. By using an upper bound on the coefficients of the j-invariant obtained from [Mah74], we derive that $\log ||C|| = O(|d_N|^{\frac{3}{2}})$. Combining this information together and taking into account the fact that $d_N = O(N \ln N)$, we obtain that the time complexity of *Poly Relation* is $O((N \ln N)^{\frac{15}{2}+o(1)})$. Similarly, its space complexity is $O((N \ln N)^{\frac{11}{2}})$.

We show a table of critical j-polynomials computed using the algorithm *Poly Relation*. We use Cremona's labels [Cre] for elliptic curves in Table 1. Implementation of the algorithm and all computations in this paper are performed using the software Sage [S$^+$14].

TABLE 1. Critical polynomials for some elliptic curves with conductor smaller than 100.

E	$g(X_0(N))$	Factorization of $F_{E,j}(x)$
37a	2	$H_{-148}(x)$
37b	2	$H_{-16}(x)^2$
44a	4	$H_{-44}(x)^2$
48a	3	$F_{E,j}(x) = 1$ $(\mathrm{div}(\omega) = [\frac{1}{4}] + [\frac{3}{4}] + [\frac{1}{12}] + [\frac{7}{12}])$
67a	5	$x^8 + 1467499520383590415545083053760x^7 + \cdots$
89a	7	$H_{-356}(x)$

3. Yang pairs and the algorithm *Poly Relation-YP*

The main issue with the algorithm *Poly Relation* is efficiency. As the conductor N gets around 1000, the kernel computation in step 5 becomes impractical. So a new method is needed.

We introduce an algorithm *Poly Relation-YP* to compute critical polynomials attached to elliptic curves. The algorithm is inspired by an idea of Yifan Yang in [Yan06]. The algorithm *Poly Relation-YP* does not compute the critical j-polynomial. Instead, it computes a critical h-polynomial, where h is some non-constant modular function on $X_0(N)$ chosen within the algorithm. First we recall a lemma of Yang.

Lemma 3.1 (Yang [Yan06]). *Suppose g, h are modular functions on $X_0(N)$ with a unique pole of order m, n at the cusp $[\infty]$, respectively, such that $\gcd(m,n)=1$. Then*

(1) $\mathbb{Q}(g,h)=\mathbb{Q}(X_0(N))$.

(2) If the leading Fourier coefficients of g and h are both 1, then there is a minimal polynomial relation between g and h of form

$$y^m - x^n + \sum_{a,b\geq 0, am+bn<mn} c_{a,b}x^a y^b. \tag{3.1}$$

Definition 3.2. A pair of two nonconstant modular functions on $X_0(N)$ is said to be a *Yang pair* if they satisfy the assumptions of Lemma 3.1.

Following [Yan06], we remark that in order to find a minimal polynomial relation of a Yang pair, we can compute the Fourier expansion of $h^m - g^n$ and use products of form $g^a h^b$ to cancel the pole at $[\infty]$ until we reach zero. In practice, this approach is significantly faster than *Poly Relation*, which finds a minimal polynomial relation of two arbitrary modular functions. This gain in speed is the main motivation of introducing *Poly Relation-YP*.

Let

$$\eta = q^{\frac{1}{24}} \prod_{n\geq 1}(1-q^n)$$

be the Dedekind η function. For any positive integer d, define the function η_d as $\eta_d(z)=\eta(dz)$.

Let N be a positive integer. An *η-product of level N* is a function of the form

$$h(z)=\prod_{d|N}\eta_d(z)^{n_d}$$

where $n_d\in\mathbb{Z}$ for all $d\mid N$. The next theorem of Ligozat gives sufficient conditions for an η-product to be a modular function on $X_0(N)$.

Lemma 3.3 (Ligozat's Criterion [Lig75]). *Let $h=\prod_{d|N}\eta_d(z)^{n_d}$ be an η-product of level N. Assume the following:*

(1) $\sum_d n_d\frac{N}{d}\equiv 0 \pmod{24}$;

(2) $\sum_d n_d d\equiv 0 \pmod{24}$;

(3) $\sum_d n_d = 0$;

(4) $\prod_{d|N}(\frac{N}{d})^{n_d}\in\mathbb{Q}^2$.

Then h is a modular function on $X_0(N)$.

If $h\in\mathbb{Q}(X_0(N))$ is an η-product, then the divisor $\mathrm{div}(h)$ is supported on the cusps of $X_0(N)$. The next lemma will allow us to construct η-products with prescribed divisors.

Lemma 3.4 (Ligozat [Lig75]). *Let $N>1$ be an integer. For every positive divisor d of N, let Pd denote the divisor on $X_0(N)$ obtained by summing all cusps of denominator d. Let ϕ denote the Euler's totient function. Then there exists an explicitly computable η-product $h\in\mathbb{Q}(X_0(N))$ such that*

$$\mathrm{div}(h)=m_d(\,Pd-\phi(\gcd(d,N/d))[\infty]\,)$$

for some positive integer m_d.

Remark 3.5. By "explicitly computable" in Lemma 3.4, we mean that one can compute a set of integers $\{n_d : d \mid N\}$ that defines the η-product h with desired property. It is a fact that the order of vanishing of an η-product at any cusp of $X_0(N)$ is a linear combination of the integers n_d. So prescribing the divisor of an η-product is equivalent to giving a linear system on the variables n_d. Thus we can solve for the n_d's and obtain the q-expansion of h from the q-expansion of η.

The next proposition is a direct consequence of Lemma 3.4.

Proposition 3.6. *Let $D \geq 0$ be a divisor on $X_0(N)$ such that D is supported on the cusps. Then there exists an explicitly computable η-product $h \in \mathbb{Q}(X_0(N))$ such that* $\operatorname{div}(h)$ *is of the form $D' - m[\infty]$, where m is a positive integer and $D' \geq D$.*

Recall our notation from Section 2 that $r = j(j-1728)\frac{\omega}{\mathrm{d}j}$.

Proposition 3.7. *There exists an explicitly computable function $h \in \mathbb{Q}(X_0(N))$ such that*

(1) The functions rh and $j(j-1728)h$ form a Yang pair;

(2) $j(j-1728)h$ is zero at all cusps of $X_0(N)$ except the cusp $[\infty]$.

Proof. Let $D = \operatorname{div}_\infty(j)$. Note that the support of D is the set of all cusps. From (2.3) we have $\operatorname{div}_\infty(r) \leq D$, $\operatorname{div}(j(j-1728)) = 2D$, $\operatorname{ord}_{[\infty]}(D) = 1$, and $\operatorname{ord}_{[\infty]}(r) = 0$. Applying Proposition 3.6 to the divisor $D_1 = 4(D - [\infty])$, we obtain an η-product $h \in \mathbb{Q}(X_0(N))$ such that $\operatorname{div}(h) = D_1' - m[\infty]$, where $D_1' \geq D_1$ and $m \geq 0$. Then $\operatorname{div}_\infty(rh) = m[\infty]$ and $\operatorname{div}_\infty(j(j-1728)h) = (m+2)[\infty]$. If m is odd, then $\gcd(m, m+2) = 1$ and (1) follows. Otherwise, we can replace h by jh. Then a similar argument shows that rh and $j(j-1728)h$ have a unique pole at $[\infty]$ and have degree $m+1$ and $m+3$, respectively. Since m is even in this case, we have $\gcd(m+1, m+3) = 1$ and (1) holds.

What we just showed is the existence of an η-product $h \in \mathbb{Q}(X_0(N))$ s.t. either h or jh satisfies (1). Now (2) follows from the fact that $\operatorname{div}_0(j(j-1728)h) > 2(D - [\infty])$ and $\operatorname{div}_0(j^2(j-1728)h) > (D - [\infty])$. □

Let h be a modular function that satisfies the conditions of Proposition 3.7. The next theorem allows us to compute $F_{E,j(j-1728)h}(x)$. For ease of notation, let $\tilde{r} = rh$ and $\tilde{h} = j(j-1728)h$.

Theorem 3.8. *Suppose h is a modular function on $X_0(N)$ that satisfies the conditions in Proposition* 3.7*. Let $P(x,y)$ be a minimal polynomial relation of $\tilde{r}$ and $\tilde{h}$ of form* (3.1)*. Write $P(x,y) = f_n(y)x^n + \cdots + f_1(y)x + f_0(y)$, and let g be the genus of $X_0(N)$; then*

$$F_{E,\tilde{h}}(x) = x^{2g-2-\deg h} f_0(x).$$

Proof. The idea is to apply Proposition 2.2 to the Yang pair $(\tilde{r}, \tilde{h})$. By Lemma 3.1, every Yang pair satisfies its first assumption. To see that the second assumption holds, observe that $f_n(y) = -1$ in (3.1), so $\gcd(f_n(y), f_0(y)) = 1$. Hence we can apply Proposition 2.2 and obtain

$$f_0(y) = \prod_{z \in \operatorname{div}_0(\tilde{r}) \setminus \operatorname{div}_\infty(\tilde{h})} (y - \tilde{h}(z))^{n_z}.$$

By construction of h, there is a divisor $D \geq 0$ on $X_0(N)$ supported on the finite set $j^{-1}(\{0, 1728\}) \cup h^{-1}(0)$ such that $\operatorname{div}(rh) = \operatorname{div}(\omega) + D - (\deg h)[\infty]$. Taking

degrees on both sides shows $\deg D = \deg h - (2g-2)$. Since $\tilde{h}(z) = 0$ for all $z \in \operatorname{supp} D$, we obtain

$$f_0(x) = F_{E,\tilde{h}}(x) \cdot x^{\deg h - 2g + 2}.$$

Dividing both sides by $x^{\deg h - 2g + 2}$ gives the desired formula. □

Next we describe the algorithm *Poly Relation-YP*.

Algorithm 2 *Poly Relation-YP*

Input: E = elliptic curve over $\mathbb{Q}$, N = conductor of E, f = the newform attached to E, g = genus of $X_0(N)$.

Output: A nonconstant modular function h on $X_0(N)$ and the critical $\tilde{h}$-polynomial $F_{E,\tilde{h}}$, where $\tilde{h} = j(j-1728)h$.

1: Find an η-product h that satisfies the conditions in Proposition 3.7.
2: $\tilde{r} := j(j-1728)h\frac{f}{j'}$, $\tilde{h} := j(j-1728)h$.
3: $M := (\deg \tilde{r} + 1)(\deg \tilde{h} + 1)$.
4: Compute q-expansions of $\tilde{r}$, $\tilde{h}$ to q^M.
5: Compute a minimal polynomial relation $P(x, y)$ of form (3.1) using the method mentioned after Lemma 3.1.
6: Output $F_{E,\tilde{h}}(x) = x^{2g-2-\deg h} P(0, x)$.

Remark 3.9. The functions $\tilde{r}$ and $\tilde{h}$ in the above algorithm are constructed in order that Theorem 3.8 has a nice and short statement. However, their degrees are large, which is not optimal for computational purposes. In practice, one can make different choices of two modular functions with smaller degrees to speed up the computation. This idea is illustrated in the following example.

Example 3.10. Let E be the elliptic curve

$$E : y^2 = x^3 - 7x + 10$$

labeled as **664a** in Cremona's table. Then $r_{\mathrm{an}}(E) = 2$, and $X_0(664)$ has genus 81. Let $r = r_4$ be as defined in Remark 2.10. Using the method described in Remark 3.5, we find two η-products:

$$h_1 = (\eta_2)^{-4}(\eta_4)^6(\eta_8)^4(\eta_{332})^6(\eta_{664})^{-12},$$
$$h_2 = (\eta_2)^{-1}(\eta_4)(\eta_{166})^{-1}(\eta_8)^2(\eta_{332})^5(\eta_{664})^{-6}$$

with the following properties: $h_1, h_2 \in \mathbb{Q}(X_0(N))$, $\operatorname{div}(rh_1) = \operatorname{div}(\omega) + D - 247[\infty]$, where $D \geq 0$ is supported on cusps, and $\operatorname{div}(h_2) = 21[1/332] + 61[1/8] + 21[1/4] - 103[\infty]$. Since (247,103) =1, the functions rh_1 and h_2 form a Yang pair. We then compute

$$F_{E,h_2}(x) = x^{160} - 1443491497715558443975973096765345920086503212026560026755519644 4x^{158} + \cdots.$$

The polynomial F_{E,h_2} is irreducible in $\mathbb{Q}[x]$.

Remark 3.11. We discuss the complexity of the algorithm *Poly Relation-YP* under the assumption that we have made good choices of $\tilde{r}$ and $\tilde{h}$ so that they have small degrees. The dominant step here is step 6, where a Laurent series is iteratively subtracted by a series of form $c\tilde{r}^a\tilde{h}^b$ until its principal part is zero. The number of iterations is $O(M) = O(N^2)$, and each iteration takes $O(M^2)$ integer operations. So the total number of integer operations is $O(N^6)$. Since we did not have a

systematic way to choose an optimal $\tilde{r}$ and $\tilde{h}$, we were unable to bound their coefficients and obtain a rigorous complexity bound on our algorithm. However, we observed through computation that suitable $\tilde{r}$ and $\tilde{h}$ can always be found with coefficients of bit length $O(\ln N)$. This suggests that the time complexity of *Poly Relation-YP* is $O(N^6(\ln N)^2)$.

In practice, *Poly Relation-YP* seems to be much faster than *Poly Relation*. We ran implementations of the two algorithms on the elliptic curve with label **64a**. The algorithm *Poly Relation* terminated in twenty minutes and output $F_{E,j}(x) = 1$ (because $\operatorname{div}(\omega)$ is supported on cusps in this case). The algorithm *Poly Relation-YP* terminated in less than one second and output the pair $(h, F_{E,h})$, where $h = (\eta_{32})(\eta_{16})^2(\eta_8)^{-1}(\eta_{64})^{-2}$ and $F_{E,h}(x) = x^4 + 16$.

4. The critical subgroup $E_{\mathrm{crit}}(\mathbb{Q})$

Recall the definition of the critical subgroup for an elliptic curve $E/\mathbb{Q}$:

$$E_{\mathrm{crit}}(\mathbb{Q}) = \langle \mathrm{tr}(\varphi(e)) : e \in \operatorname{supp}\operatorname{div}(\omega)\rangle.$$

Observe that to generate $E_{\mathrm{crit}}(\mathbb{Q})$, it suffices to take one representative from each Galois orbit of $\operatorname{supp}\operatorname{div}(\omega)$. Therefore, if we let n_ω denote the number of Galois orbits in $\operatorname{div}(\omega)$, then

$$\operatorname{rank}(E_{\mathrm{crit}}(\mathbb{Q})) \le n_\omega.$$

For any rational divisor $D = \sum_{[z]\in X_0(N)} n_z[z]$ on $X_0(N)$, let

$$p_D = \sum_{z\in\operatorname{supp} D} n_z\varphi([z]);$$

then $p_D \in E(\mathbb{Q})$. Note that $p_D = 0$ if D is a principal divisor. The point $p_{\operatorname{div}(\omega)}$ is a linear combination of the defining generators of $E_{\mathrm{crit}}(\mathbb{Q})$.

Lemma 4.1. $6\,p_{\operatorname{div}(\omega)} \equiv -3\sum_{c\in\mathcal{E}_2(N)}\varphi(c) - 4\sum_{d\in\mathcal{E}_3(N)}\varphi(d) \pmod{E(\mathbb{Q})_{\mathrm{tors}}}$.

Proof. Let $r_0 = \omega/\operatorname{d}j$. Then $r_0 \in \mathbb{Q}(X_0(N))$; hence $p_{\operatorname{div}(r_0)} = 0$. From $\operatorname{div}(r_0) = \operatorname{div}(\omega) - \operatorname{div}(\operatorname{d}j)$, we deduce that $p_{\operatorname{div}(\omega)} = p_{\operatorname{div}(\operatorname{d}j)}$. The lemma then follows from the formula of $\operatorname{div}(\operatorname{d}j)$ given in (2.2) and the fact that the image of any cusp under φ is torsion. □

Proposition 4.2. *Assume at least one of the following holds:*
(1) $r_{\mathrm{an}}(E) \ge 2$*;*
(2) $X_0(N)$ *has no elliptic point.*
Then $\operatorname{rank}(E_{\mathrm{crit}}(\mathbb{Q})) \le n_\omega - 1$.

Proof. By Lemma 4.1 and Theorem 1.3, either assumption implies that $p_{\operatorname{div}(\omega)}$ is torsion. But $p_{\operatorname{div}(\omega)}$ is a linear combination of the n_ω generators of $E_{\mathrm{crit}}(\mathbb{Q})$, so these generators are linearly dependent in $E_{\mathrm{crit}}(\mathbb{Q})\otimes\mathbb{Q}$. Hence the rank of $E_{\mathrm{crit}}(\mathbb{Q})$ is smaller than n_ω. □

Now we are ready to prove Theorem 1.6.

Proof of Theorem 1.6. First, note that the definition of $F_{E,j}$ only involves critical points that are not cusps. However, since images of cusps under φ are torsion,

we can replace $\mathrm{div}(\omega)$ by $\mathrm{div}(\omega) \setminus \{\text{cusps of } X_0(N)\}$ if necessary and assume that $\mathrm{div}(\omega)$ does not contain cusps.

(1) If $F_{E,h}$ is irreducible, then we necessarily have $n_\omega = 1$, and the claim follows from Proposition 4.2.

(2) Let $d = \deg F_0$. Then there exists a Galois orbit in $\mathrm{div}(\omega)$ of size d, and the other $(2g-2-d)$ points in $\mathrm{div}(\omega)$ are CM points. Let z be any one of the $(2g-2-d)$ points. Then $j(z)$ is a root of $H_{D_k}(x)$ and $z \in \mathbb{Q}(\sqrt{D_k})$. Since $\mathrm{div}(\omega)$ is invariant under the Fricke involution w_N, one sees that $j(Nz)$ is also a root of $F_{E,j}$. Therefore, $j(Nz)$ is the root of $H_{D_{k'}}(x)$ for some $1 \le k' \le m$. Since z and Nz define the same quadratic field, we must have $\mathbb{Q}(\sqrt{D_k}) = \mathbb{Q}(\sqrt{D_{k'}})$, which implies $k = k'$ by our assumption. It follows that $[z]$ is a "generalized Heegner point" (defined in Definition 1.2) and $\mathrm{tr}(\varphi([z]))$ is torsion. By the form of $F_{E,j}$, there exists a point $[z_0] \in \mathrm{supp}\,\mathrm{div}(\omega)$ such that $j(z_0)$ is a root of F_0. Then we have $\mathrm{rank}(E_{\mathrm{crit}}(\mathbb{Q})) = \mathrm{rank}(\langle \mathrm{tr}(\varphi([z_0]))\rangle) = \mathrm{rank}(\langle p_{\mathrm{div}(\omega)}\rangle)$. Finally, Lemma 4.1 implies $\mathrm{rank}(\langle p_{\mathrm{div}(\omega)}\rangle) = 0$, and it follows that $\mathrm{rank}(E_{\mathrm{crit}}(\mathbb{Q})) = 0$.

Remark 4.3. Christophe Delaunay has an algorithm to compute $\mathrm{div}(\omega)$ numerically as equivalence classes of points in the upper half plane (see [Del02] and [Del05]). A table of critical points for the elliptic curve

$$E : y^2 + y = x^3 + x^2 - 2x$$

with rank two and Cremona label **389a** is presented in [Del02, Appendix B.1]. The results suggest that $\mathrm{div}(\omega)$ contains two Heegner points of discriminant 19, and the critical subgroup $E_{\mathrm{crit}}(\mathbb{Q})$ is torsion. Using the critical j-polynomial for **389a** in Table 2, we can confirm the numerical results of Delaunay.

5. Data

5.1. **Rank one elliptic curves.** When $r_{\mathrm{an}}(E) = 1$, the rank of $E_{\mathrm{crit}}(\mathbb{Q})$ is either zero or one. In fact, both cases occur.

Example 5.1. Consider the elliptic curve

$$E : y^2 + y = x^3 - x^2 + x$$

with label **131a**. Then $r_{\mathrm{an}}(E) = 1$ and the modular degree of E is 2. Hence we have $E \cong X_0(131)/W_{131}$, where W_{131} is the Fricke involution on $X_0(131)$, and $\mathrm{supp}\, R_\varphi$ is precisely the set of fixed points of W_{131} on $X_0(131)$. A computation shows that $E_{\mathrm{crit}}(\mathbb{Q}) = 0$.

Example 5.1 is related to the fact that the quadratic twist E_{-131} of E has analytic rank two. In fact, if $r_{\mathrm{an}}(E) = 1$, then φ factors through the map $X_0(N) \to X_0(N)/W_N$, so $\mathrm{supp}\, R_\varphi$ contains the fixed points of W_N. If the twist E_{-N} has analytic rank zero, then these fixed points give rise to a rank one subgroup in $E_{\mathrm{crit}}(\mathbb{Q})$, which implies $\mathrm{rank}(E_{\mathrm{crit}}(\mathbb{Q})) = 1$.

Example 5.2. Let E be the elliptic curve with Cremona label **197a**. Then $r_{\mathrm{an}}(E) = 1$, and we compute

$$F_{E,j} = (x + 884736)^2 H_{-788}(x) F_0,$$

where $F_0 \in \mathbb{Q}[x]$ is irreducible of degree 18. From the linear factors of $F_{E,j}$ we deduce that $\mathrm{div}(\omega)$ contains the two Heegner points

$$z_1 = \frac{1}{394}\sqrt{19}i - \frac{93}{394}, \qquad z_2 = \frac{1}{394}\sqrt{19}i - \frac{301}{394}$$

of discriminant 19 on $X_0(197)$. It turns out that $\mathrm{tr}(\varphi(z_i))$ generates $E(\mathbb{Q})$ for each $i = 1, 2$, so we have $E_{\mathrm{crit}}(\mathbb{Q}) = E(\mathbb{Q})$.

5.2. **Rank two elliptic curves.** The columns of Table 2 are as follows. The column labeled E contains labels of elliptic curves, and the column labeled g contains the genus of $X_0(N)$, where N is the conductor of E. The column labeled h contains a modular function on $X_0(N)$: either the j-invariant or some η-product. Note that we choose $h = j$ whenever computing $F_{E,j}$ takes reasonable time, because it is easier to identify "generalized Heegner points" occurring in $\mathrm{div}(\omega)$ by observing Hilbert class polynomials in the factorization of $F_{E,j}$. The last column contains the factorization of the critical h-polynomial of E defined in Section 1.2 for our choice of h. The factors of $F_{E,j}$ that are Hilbert class polynomials are written out explicitly. Table 2 contains *all* elliptic curves with conductor $N < 1000$ and rank two. By observing that each critical polynomial in the table satisfies the assumptions of Theorem 1.6, we obtain Corollary 1.7.

TABLE 2. Critical polynomials for elliptic curves of rank two and conductor smaller than 1000.

E	$g(X_0(N))$	h	Factorization of $F_{E,h}(x)$
389a	32	j	$H_{-19}(x)^2(x^{60} + \cdots)$
433a	35	j	$x^{68} + \cdots$
446d	55	j	$x^{108} + \cdots$
563a	47	j	$H_{-43}(x)^2(x^{90} - \cdots)$
571b	47	j	$H_{-67}(x)^2(x^{90} - \cdots)$
643a	53	j	$H_{-19}(x)^2(x^{102} - \cdots)$
664a	81	$\frac{\eta_4\eta_8^2\eta_{332}^5}{\eta_{166}\eta_{664}^6\eta_2}$	$x^{160} - \cdots$
655a	65	j	$x^{128} - \cdots$
681c	75	j	$x^{148} - \cdots$
707a	67	j	$x^{132} - \cdots$
709a	58	j	$x^{114} - \cdots$
718b	89	j	$H_{-52}(x)^2(x^{172} - \cdots)$
794a	98	j	$H_{-4}(x)^2(x^{192} - \cdots)$
817a	71	j	$x^{140} - \cdots$
916c	113	j	$H_{-12}(x)^8(x^{216} + \cdots)$
944e	115	$\frac{\eta_{16}^4\eta_4^2}{\eta_8^6}$	$x^{224} - \cdots$
997b	82	j	$H_{-27}(x)^2(x^{160} - \cdots)$
997c	82	j	$x^{162} - \cdots$

5.3. **Rank three elliptic curves?** Unfortunately, our current algorithms fail to compute the critical subgroup of the first rank three elliptic curve, which has Cremona label **5077a**. In fact, any critical polynomial $F_{E,h}$ for this curve will have degree 842 and potentially huge coefficients, which suggests that it is hard to compute using our methods.

5.4. **Further questions.** From our computation, it seems hard to find an elliptic curve $E/\mathbb{Q}$ with $r_{\mathrm{an}}(E) \geq 2$ and $\mathrm{rank}(E_{\mathrm{crit}}(\mathbb{Q})) > 0$. Nonetheless, some interesting questions can be raised.

Question 5.3. For all elliptic curves $E/\mathbb{Q}$, does $F_{E,j}$ always factor in $\mathbb{Q}[x]$ as a product of Hilbert class polynomials and one irreducible polynomial?

If the answer to Question 5.3 is positive, then we would know $E_{\mathrm{crit}}(\mathbb{Q})$ is torsion whenever $r_{\mathrm{an}}(E) \geq 2$.

Another way to construct rational points on E is to take any nonzero cusp form $l(z) \in S_2(\Gamma_0(N), \mathbb{Z})$ and let $E_l(\mathbb{Q}) = \langle \mathrm{tr}(\varphi([z])) : [z] \in \mathrm{supp}\,\mathrm{div}(l(z)dz) \rangle$.

Question 5.4. Does there exist $l(z) \in S_2(\Gamma_0(N), \mathbb{Z})$ such that $E_l(\mathbb{Q})$ is non-torsion?

Remark 5.5. Consider the irreducible factors of $F_{E,j}$ that are *not* Hilbert class polynomials. It turns out that their constant terms have many small prime factors, a property also enjoyed by Hilbert class polynomials. For example, consider the polynomial $F_{67a,j}$. It is irreducible and not equal to any Hilbert class polynomial, while its constant term has factorization

$$2^{68} \cdot 3^2 \cdot 5^3 \cdot 23^6 \cdot 443^3 \cdot 186145963^3.$$

It is interesting to investigate the properties of these polynomials.

Remark 5.6. In [MSD74], the authors defined *fundamental critical points* of an elliptic curve E as points in $\mathrm{supp}\,\mathrm{div}(\omega)$ that has real part zero. Then they proved that the number of fundamental critical points of E, counting multiplicity, is an upper bound of $r_{\mathrm{an}}(E)$. We computed the fundamental critical points numerically for the curves in Table 2. It seems that for each curve in Table 2, there are two fundamental critical points, and both belong to the single Galois orbit in $\mathrm{div}(\omega)$ that does not contain "generalized Heegner points".

For the curve **5077a**, numerical computation suggests that it has three fundamental critical points: $z_1 = [\frac{i}{\sqrt{5077}}]$, $z_2 \approx [0.34568948542043501671i]$, and $z_3 = W_N(z_2)$. Since z_1 is a "generalized Heegner point" on a rank three curve, we know $\mathrm{tr}(\varphi(z_1))$ is torsion. We are not sure yet whether $\mathrm{tr}(\varphi(z_2))$ has infinite order.

Remark 5.7. The polynomial relation $P(x, y)$ between r and u can be applied to other computational problems regarding modular forms attached to elliptic curves. For example, one could use it for the computation of q-expansions of newforms at all cusps (see upcoming paper [Che]).

Acknowledgment

The author is indebted to John Voight for helpful discussions in the course of this work.

References

[AO03] S. Ahlgren and K. Ono, *Weierstrass points on $X_0(p)$ and supersingular j-invariants*, Math. Ann. **325** (2003), no. 2, 355–368, DOI 10.1007/s00208-002-0390-9. MR1962053 (2004b:11086)

[BCDT01] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939 (electronic), DOI 10.1090/S0894-0347-01-00370-8. MR1839918 (2002d:11058)

[BFH90] D. Bump, S. Friedberg, and J. Hoffstein, *Nonvanishing theorems for L-functions of modular forms and their derivatives*, Invent. Math. **102** (1990), no. 3, 543–618, DOI 10.1007/BF01233440. MR1074487 (92a:11058)

[Che] Hao Chen, *Computing Fourier expansion of* $\Gamma_0(N)$ *newforms at non-unitary cusps*, in preparation.

[Cre] J. E. Cremona, *Elliptic curve data*, `http://www.maths.nott.ac.uk/personal/jec/ftp/data/INDEX.html`.

[Del02] Christophe Delaunay, *Formes modulaires et invariants de courbes elliptiques définies sur* $\mathbb{Q}$, Thèse de doctorat, Université Bordeaux 1 (décembre 2002).

[Del05] C. Delaunay, *Critical and ramification points of the modular parametrization of an elliptic curve* (English, with English and French summaries), J. Théor. Nombres Bordeaux **17** (2005), no. 1, 109–124. MR2152214 (2006c:11075)

[GZ86] B. H. Gross and D. B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320, DOI 10.1007/BF01388809. MR833192 (87j:11057)

[Lig75] G. Ligozat, *Courbes modulaires de genre* 1 (French), 1975. Bull. Soc. Math. France, Mém. 43; Supplément au Bull. Soc. Math. France Tome 103, no. 3, Société Mathématique de France, Paris. MR0417060 (54 #5121)

[Mah74] K. Mahler, *On the coefficients of transformation polynomials for the modular function*, Bull. Austral. Math. Soc. **10** (1974), 197–218. MR0354556 (50 #7034)

[MS04] T. Mulders and A. Storjohann, *Certified dense linear system solving*, J. Symbolic Comput. **37** (2004), no. 4, 485–510, DOI 10.1016/j.jsc.2003.07.004. MR2093448 (2006c:11151)

[MSD74] B. Mazur and P. Swinnerton-Dyer, *Arithmetic of Weil curves*, Invent. Math. **25** (1974), 1–61. MR0354674 (50 #7152)

[S$^+$14] W. A. Stein et al., *Sage Mathematics Software (Version 6.4)*, The Sage Development Team, 2014, `http://www.sagemath.org`.

[Ste] William Stein, *Algebraic number theory, a computational approach*, `https://github.com/williamstein/ant`.

[Yan06] Y. Yang, *Defining equations of modular curves*, Adv. Math. **204** (2006), no. 2, 481–508, DOI 10.1016/j.aim.2005.05.019. MR2249621 (2007e:11068)

Department of Mathematics, University of Washington, Seattle, Washington 98115
E-mail address: `chenh123@uw.edu`