The Modular Curve $X_0(389)$:

Discriminants, Ranks, Shafarevich-Tate Groups, and Weierstrass Points

William Stein

April 2002

1 Introduction

Let N be a positive integer, and let $X_0(N)$ be the compactified coarse moduli space that classifies pairs (E, C) where E is an elliptic curve and C is a cyclic subgroup of order N. The space $X_0(N)$ has a canonical structure of algebraic curve over $\mathbb{Q}$, and its properties have been very well studied during the last forty years. For example, Breuil, Conrad, Diamond, Taylor, and Wiles proved that every elliptic curve over $\mathbb{Q}$ is a quotient of some $X_0(N)$.

The smallest N such that the Jacobian of $X_0(N)$ has positive Mordell-Weil rank is 37, and Zagier studied the genus-two curve $X_0(37)$ in depth in his paper [18]. From this viewpoint, the next modular curve deserving intensive investigation is $X_0(389)$, which is the first modular curve whose Jacobian has Mordell-Weil rank larger than that predicted by the signs in the functional equations of the L-series attached to simple factors of its Jacobian; in fact, 389 is the smallest conductor of an elliptic curve with Mordell-Weil rank 2. Note that 389 is prime and $X_0(389)$ has genus $g = 32$, which is much larger than the genus 2 of $X_0(37)$, which makes explicit investigation more challenging.

Work of Kolyvagin [9, 8] and Gross-Zagier [7] has completely resolved the rank assertion of the Birch and Swinnerton-Dyer conjecture (see, e.g., [17]) for elliptic curves E with $\mathrm{ord}_{s=1} L(E, s) \leq 1$. The lowest-conductor elliptic curve E that doesn't submit to the work of Kolyvagin and Gross-Zagier is the elliptic curve E of conductor 389 mentioned in the previous paragraph. At present we don't even have a conjectural natural construction of a finite-index subgroup of $E(\mathbb{Q})$ analogous to that given by Gross and Zagier for rank 1 (but see Mazur's work on universal norms, which might be used to construct $E(\mathbb{Q}) \otimes \mathbb{Z}_p$ for some auxiliary prime p).

Inspired by the above observations, and with an eye towards providing helpful data for anyone trying to generalize the work of Gross, Zagier, and Kolyvagin, in this paper we compute everything we can about the modular curve $X_0(389)$. Some of the computations of this paper have already proved important in several other papers: the discriminant of the Hecke algebra attached to $X_0(389)$ plays a roll in

[14], the verification of condition 3 in [11], and the remark after Theorem 1 of [10]; also, the arithmetic of $J_0(389)$ provides a key example in [3, §4.2]. Finally, this paper serves as an entry in an "encyclopaedia, atlas or hiker's guide to modular curves", in the spirit of N. Elkies (see [5, pg. 22]).

We hilight several surprising "firsts" that occur at level 389. The discriminant of the Hecke algebra attached to $S_2(\Gamma_0(389))$ has the apparently unusual property that it is divisible by $p = 389$ (see Section 3.1). Also $N = 389$ is the smallest integer such that the order of vanishing of $L(J_0(N), s)$ at $s = 1$ is larger than predicted by the functional equations of eigenforms (see Section 2.3). The author conjectures that $N = 389$ is the smallest level such that an optimal newform factor of $J_0(N)$ appears to have Shafarevich-Tate group with nontrivial odd part (see Section 5.1). Atkin conjectures that 389 is the largest prime such that the cusp of $X_0^+(389)$ fails to be a Weierstrass point (see Section 5.2).

Acknowledgement. Noam Elkies, Ken Ribet, Matt Baker. Hendrik Lenstra, for suggesting a method to compute discriminants of Hecke algebra efficiently (see Section 3).

2 Factors of $J_0(389)$

To each newform $f \in S_2(\Gamma_0(389))$, Shimura [16] associated a quotient A_f of $J_0(389)$, and $J_0(389)$ is isogeneous to the product $\prod A_f$, where the product runs over the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugacy classes of newforms. Moreover, because 389 is prime each factor A_f cannot be decomposed further up to isogeny, even over $\overline{\mathbb{Q}}$ (see [13]).

2.1 Newforms of Level 389

There are five $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugacy classes of newforms in $S_2(\Gamma_0(389))$. The first class corresponds to the unique elliptic curve of conductor 389, and its q-exansion begins

$$f_1 = q - 2q^2 - 2q^3 + 2q^4 - 3q^5 + 4q^6 - 5q^7 + q^9 + 6q^{10} + \cdots .$$

The second has coefficients in the quadratic field $\mathbb{Q}(\sqrt{2})$, and has q-expansion

$$f_2 = q + \sqrt{2}q^2 + (\sqrt{2} - 2)q^3 - q^5 + (-2\sqrt{2} + 2)q^6 + \cdots .$$

The third has coefficients in the cubic field generated by a root α of $x^3 - 4x - 2$:

$$f_3 = q + \alpha q^2 - \alpha q^3 + (\alpha^2 - 2)q^4 + (-\alpha^2 + 1)q^5 - \alpha^2 q^6 + \cdots .$$

The fourth has coefficients that generate the degree-six field defined by a root β of $x^6 + 3x^5 - 2x^4 - 8x^3 + 2x^2 + 4x - 1$ and q-expansion

$$f_4 = q + \beta q^2 + (\beta^5 + 3\beta^4 - 2\beta^3 - 8\beta^2 + \beta + 2)q^3 + \cdots .$$

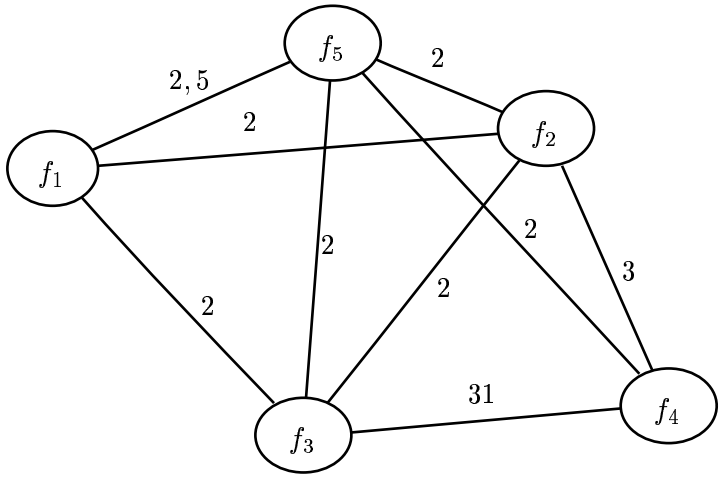

Figure 2.1: Congruences Between Newforms

The fifth and final newform (up to conjugacy) has coefficients that generate the degree 20 field defined by a root of

$$\begin{aligned} f_5 \;=\; & x^{20} - 3x^{19} - 29x^{18} + 91x^{17} + 338x^{16} - 1130x^{15} - 2023x^{14} + 7432x^{13} \\ & +6558x^{12} - 28021x^{11} - 10909x^{10} + 61267x^9 + 6954x^8 - 74752x^7 \\ & +1407x^6 + 46330x^5 - 1087x^4 - 12558x^3 - 942x^2 + 960x + 148. \end{aligned}$$

2.1.1 Congruences

The vertices in Figure 2.1 correspond to the newforms f_i; there is an edge between f_i and f_j labeled p if there is a maximal ideal $\wp \mid p$ of the field generated by the Fourier coefficients of f_i and f_j such that $f_i \equiv f_j \pmod{\wp}$.

2.2 Isogeny Structure

We deduce from the above determination of the newforms in $S_2(\Gamma_0(389))$ that $J_0(389)$ is $\mathbb{Q}$-isogenous to a product of $\overline{\mathbb{Q}}$-simple abelian varieties

$$J \sim A_1 \times A_2 \times A_3 \times A_4 \times A_5.$$

View the duals $A_i^\vee$ of the A_i as abelian subvarieties of $J_0(389)$. Using modular symbols as in [2, §3.4] we find that, for $i \neq j$, a prime p divides $\#(A_i^\vee \cap A_j^\vee)$ if and only if $f_i \equiv f_j \pmod{\wp}$ for some prime $\wp \mid p$ (recall that the congruence primes are given in Figure 2.1 above).

2.3 Mordell-Weil Ranks

Suppose $f \in S_2(\Gamma_0(N))$ is a newform of some level N. The functional equation for $L(f,s)$ implies that $\mathrm{ord}_{s=1} L(f,s)$ is odd if and only if the sign of the eigenvalue of the Atkin-Lehner involution W_N on f is $+1$.

Proposition 2.1. *If $f \in S_2(\Gamma_0(N))$ is a newform of level $N < 389$, then $\mathrm{ord}_{s=1} L(f,s)$ is either 0 or 1.*

Proof. The proof amounts to a large computation, which divides into two parts:

1. Verify, for each newform f of level $N < 389$ such that $W_N(f) = -f$, that $L(f,1) = * \int_0^{i\infty} f(z)dz$ (for some nonzero $*$) is nonzero. This is a purely algebraic computation involving modular symbols.

2. Verify, for each newform f of level $N < 389$ such that $W_N(f) = f$, that $L'(f,1) \neq 0$ (see [6, §4.1], which points to [4, §2.11,§2.13]). We do this by approximating an infinite series that converges to $L'(f,1)$ and noting that the value we get is far from 0.

□

Thus $N = 389$ is the smallest level such that the L-series of some factor A_f of $J_0(N)$ has order of vanishing higher than that which is forced by the sign in the functional equation.

Proposition 2.2. *The following table summarizes the dimensions and Mordell-Weil ranks (over the image of the Hecke ring) of the newform factors of $J_0(N)$:*

	A_1	A_2	A_3	A_4	A_5
Dimension	1	2	3	6	20
Rank	2	1	1	1	0

Proof. The elliptic curve A_1 is $389A$ in Cremona's tables, which is the elliptic curve of smallest conductor having rank 2. For A_5 we directly compute whether or not the L-function vanishes using modular symbols, by taking an inner product with the winding element $e_w = -\{0,\infty\}$. We find that the L-function does not vanish. By Kolyvagin-Logachev, it follows that A_5 has Mordell-Weil rank 0.

For each of the other three factors, the sign of the functional equation is odd, so the analytic ranks are odd. As in the proof of Proposition 2.1, we verify that the analytic rank is 1 in each case. By work of Gross, Zagier, and Kolyvagin it follows that the ranks are 1. □

3 The Hecke algebra

3.1 The Discriminant is Divisible By p

Let N be a positive integer. The Hecke algebra $\mathbf{T} \subset \mathrm{End}(S_2(\Gamma_0(N)))$ is the subring generated by all Hecke operators T_n for $n = 1, 2, 3, \ldots$. We are concerned with the *discriminant* of the trace pairing $(t, s) \mapsto \mathrm{Tr}(ts)$.

When N is prime, $\mathbf{T}_{\mathbb{Q}} = \mathbf{T} \otimes_{\mathbb{Z}} \mathbb{Q}$ is a product $K_1 \times \cdots \times K_n$ of totally real number fields. Let $\tilde{\mathbf{T}}$ denote the integral closure of $\mathbf{T}$ in $\mathbf{T}_{\mathbb{Q}}$; note that $\tilde{\mathbf{T}} = \prod \mathcal{O}_i$ where $\mathcal{O}_i$ is the ring of integers of K_i. Then $\mathrm{disc}(\mathbf{T}) = [\tilde{\mathbf{T}} : \mathbf{T}] \cdot \prod_{i=1}^{n} \mathrm{disc}(K_i)$.

Proposition 3.1. *The discriminant of the Hecke algebra associated to $S_2(\Gamma_0(389))$ is*

$$2^{53} \cdot 3^4 \cdot 5^6 \cdot 31^2 \cdot 37 \cdot 389 \cdot 3881 \cdot 215517113148241 \cdot 477439237737571441.$$

Proof. By [1], the Hecke algebra $\mathbf{T}$ is generated as a $\mathbb{Z}$-module by $T_1, T_2, \ldots T_{65}$. To compute $\mathrm{disc}(\mathbf{T})$, we proceed as follows. First, compute the space $\boldsymbol{\mathcal{S}}_2(\Gamma_0(389))$ of cuspidal modular symbols, which is a faithful $\mathbf{T}$-module. Choose a random element $x \in \boldsymbol{\mathcal{S}}_2(\Gamma_0(389))_+$ of the $+1$-quotient of the cuspidal modular symbols, then compute the images $v_1 = T_1(x), v_2 = T_2(x), \ldots, v_{65} = T_{65}(x)$. If these don't span a space of dimension $32 = \mathrm{rank}_{\mathbb{Z}} \mathbf{T}$ choose a new random element x and repeat. Using the Hermite Normal Form, find a $\mathbb{Z}$-basis $b_1, \ldots, b_{32}$ for the $\mathbb{Z}$-span of $v_1, \ldots, v_{65}$. The trace pairing on $\mathbf{T}$ induces a trace pairing on the v_i, and hence on the b_i. Then $\mathrm{disc}(\mathbf{T})$ is the discriminant of this pairing on the b_i. The reason we embed $\mathbf{T}$ in $\boldsymbol{\mathcal{S}}_2(\Gamma_0(389))_+$ as $\mathbf{T}x$ is because directly finding a $\mathbb{Z}$-basis for $\mathbf{T}$ would involve computing the Hermite Norm Form of a list of 65 vectors in a 1024-dimensional space, which is unnecessarily difficult (though possible). □

We compute this discriminant by applying the definition of discriminant to a matrix representation of the first 65 Hecke operators $T_1, \ldots, T_{65}$. Matrices representing these Hecke operators were computed using the modular symbols algorithms described in [4]. [Sturm, *On the congruence of modular forms*].

In the case of $X_0(389)$, $\mathbf{T} \otimes \mathbb{Q} = K_1 \times K_2 \times K_3 \times K_6 \times K_{20}$, where K_d has degree d over $\mathbb{Q}$. We have

$$\begin{aligned}
K_1 &= \mathbb{Q}, \\
K_2 &= \mathbb{Q}(\sqrt{2}) \\
K_3 &= \mathbb{Q}(\beta), \quad \beta^3 - 4\beta - 2 = 0, \\
K_6 &= \mathbb{Q}(\gamma), \quad \gamma^6 + 3\gamma^5 - 2\gamma^4 - 8\gamma^3 + 2\gamma^2 + 4\gamma - 1 = 0, \\
K_{20} &= \mathbb{Q}(\delta), \quad \delta^{20} - 3\delta^{19} - 29\delta^{18} + 91\delta^{17} + 338\delta^{16} - 1130\delta^{15} - 2023\delta^{14} + 7432\delta^{13} \\
&\qquad +6558\delta^{12} - 28021\delta^{11} - 10909\delta^{10} + 61267\delta^9 + 6954\delta^8 - 74752\delta^7 \\
&\qquad +1407\delta^6 + 46330\delta^5 - 1087\delta^4 - 12558\delta^3 - 942\delta^2 + 960\delta + 148 = 0.
\end{aligned}$$

The discriminants of the K_i are

K_1	K_2	K_3	K_6
1	2^3	$2^2 \cdot 37$	$5^3 \cdot 3881$

and

$$\mathrm{disc}(K_{20}) = 2^{14} \cdot 5 \cdot 389 \cdot 215517113148241 \cdot 477439237737571441.$$

Observe that the discriminant of K_{20} is divisible by 389. The product of the discriminants is

$$2^{19} \cdot 5^4 \cdot 37 \cdot 389 \cdot 3881 \cdot 215517113148241 \cdot 477439237737571441.$$

This differs from the exact discriminant by a factor of $2^{34} \cdot 3^4 \cdot 5^2 \cdot 31^2$, so the index of $\mathbf{T}$ in its normalization is

$$[\tilde{\mathbf{T}} : \mathbf{T}] = 2^{17} \cdot 3^2 \cdot 5 \cdot 31.$$

Notice that 389 does not divide this index, and that 389 is not a "congruence prime", so 389 does not divide any modular degrees.

Question 3.2. Is there a newform optimal quotient A_f of $J_0(p)$ such that p divides the modular degree of A_f? (No, if $p < 14000$.)

3.2 Congruences Primes in $S_{p+1}(\Gamma_0(1))$

K. Ono asked the following question, in connection with Theorem 1 of [10].

Question 3.3. Let p be a prime. Is p ever a congruence prime on $S_{p+1}(\Gamma_0(1))$? More precisely, if K is the number field generated by all the eigenforms of weight $p+1$ on $\Gamma_0(1)$, can there be a prime ideal $\wp \mid p$ for which $f \equiv g \pmod{\wp}$ for distinct eigenforms $f, g \in S_{p+1}(\Gamma_0(1))$?

The answer is "yes". There is a standard relationship between $S_{p+1}(\Gamma_0(1))$ and $S_2(\Gamma_0(p))$. As noted in Section 3.1, $p = 389$ is a congruence prime for $S_2(\Gamma_0(389))$, so we investigate $S_{389+1}(\Gamma_0(1))$.

Proposition 3.4. *There exist distinct newforms $f, g \in S_{389+1}(\Gamma_0(1))$ and a prime $\wp$ of residue characteristic 389 such that $f \equiv g \pmod{\wp}$.*

Proof. We compute the characteristic polynomial f of the Hecke operator T_2 on $S_{389+1}(\Gamma_0(1))$ using nothing more than [15, Ch. VII]. We find that f factors modulo 389 as follows:

$$\begin{aligned}
\overline{f} \;=\; & (x+2)(x+56)(x+135)(x+158)(x+175)^2(x+315)(x+342)(x^2+387) \\
& (x^2+97x+164)(x^2+231x+64)(x^2+286x+63) \\
& (x^5+88x^4+196x^3+113x^2+168x+349) \\
& (x^{11}+276x^{10}+182x^9+13x^8+298x^7+316x^6+213x^5 \\
& \quad +248x^4+108x^3+283x^2+x+101)
\end{aligned}$$

Moreover, f is irreducible and $389 \mid\mid \mathrm{disc}(f)$, so the square factor $(x+175)^2$ implies that 389 is ramified in the degree-32 field L generated by a single root of f. Thus there are exactly 31 distinct homomorphisms from the ring of integers of L to $\overline{\mathbb{F}}_{389}$. That is, there are exactly 31 ways to reduce the q-expansion of a newform in $S_{390}(\Gamma_0(1))$ to obtain a q-expansion in $\overline{\mathbb{F}}_{389}[[q]]$. Let K be the field generated by all eigenvalues of the 32 newforms $g_1, \ldots g_{32} \in S_{390}(\Gamma_0(1))$, and let $\wp$ be a prime of $\mathcal{O}_K$ lying over 389. Then the subset $\{g_1 \pmod{\wp}, g_2 \pmod{\wp}, \ldots, g_{32} \pmod{\wp}\}$ of $\overline{\mathbb{F}}_{389}[[q]]$ has cardinality at most 31, so there exists $i \neq j$ such that $g_i \equiv g_j \pmod{\wp}$. □

4 Supersingular Points in Characteristic 389

4.1 The Supersingular j-invariants In Characteristic 389

Let α be a root of $\alpha^2 + 95\alpha + 20$. Then the $33 = g(X_0(389)) + 1$ supersingular j-invariants in $\mathbb{F}_{389^2}$ are

$$0, 7, 16, 17, 36, 121, 154, 220, 318, 327, 358, 60\alpha + 22, 68\alpha + 166, 80\alpha + 91, 86\alpha + 273,$$
$$93\alpha + 333, 123\alpha + 350, 123\alpha + 375, 129\alpha + 247, 131\alpha + 151, 160\alpha + 321, 176\alpha + 188,$$
$$213\alpha + 195, 229\alpha + 292, 258\alpha + 154, 260\alpha + 51, 266\alpha + 335, 266\alpha + 360, 296\alpha + 56,$$
$$303\alpha + 272, 309\alpha + 271, 321\alpha + 319, 329\alpha + 157.$$

Figure 4.1 contains the graph of the Hecke operator T_2 computed using method of Mestre and Oesterlé [12]. Here, if $T_2(j) = \sum_i j_i$, then there is an edge from the node j to each of the nodes j_i. Thus, for example,

$$T_2([318]) = [0] + [93\alpha + 333] + [296\alpha + 56].$$

4.2 Gross Triple-Product Business

5 Miscellaneous

5.1 The Shafarevich-Tate Group

Using visibility theory [3, §4.2], one sees that $\#Ш(A_5)$ is divisible by an odd prime, because

$$(\mathbb{Z}/5\mathbb{Z})^2 \approx A_1(\mathbb{Q})/5A_1(\mathbb{Q}) \subset Ш(A_5).$$

Additional computations suggest the following conjecture.

Conjecture 5.1. *$N = 389$ is the smallest level such that there is an optimal newform quotient A_f of $J_0(N)$ with $\#Ш(A_f)$ divisible by an odd prime.*

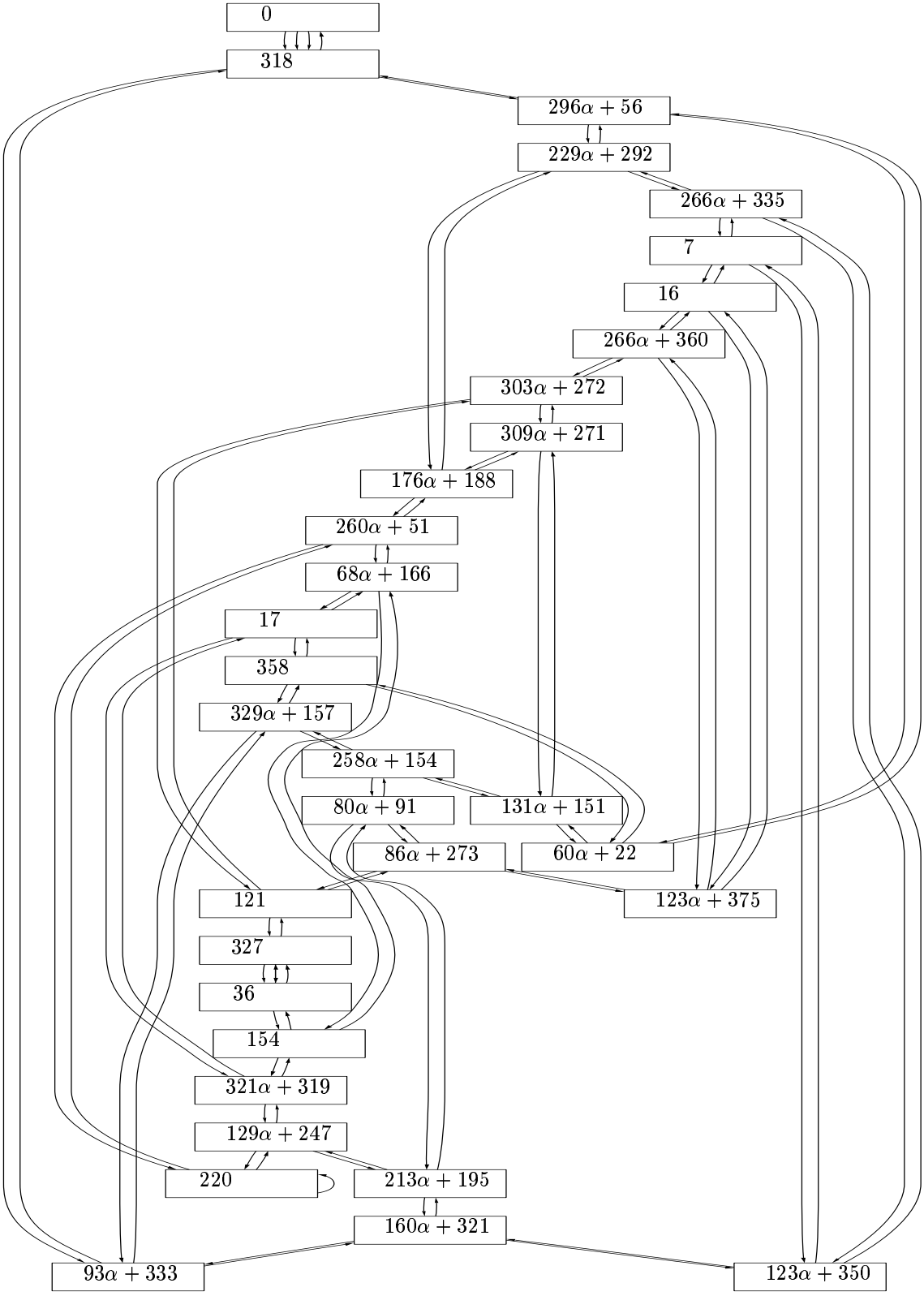

Figure 4.1: Graph of the Hecke Operator T_2

5.2 Weierstrass Points on $X_0^+(p)$

Oliver Atkin has conjectured that 389 is the largest prime such that the cusp on $X_0^+(389)$ fails to be a Weierstrass point. He verified that the cusp of $X_0^+(389)$ is not a Weierstrass point but that the cusp of $X_0^+(p)$ is a Weierstrass point for all primes p such that $389 < p \leq 883$ (see, e.g., [5, pg.39]). In addition, the author has extended the verification of Atkin's conjecture for all primes < 3000. Explicitly, this involves computing a reduced-echelon basis for the subspace of $S_2(\Gamma_0(p))$ where the Atkin-Lehner involution W_p acts as $+1$, and comparing the largest valuation of an element of this basis with the dimension of the subspace. These numbers differ exactly when the cusp is a Weierstrass point.

5.3 A Property of the Plus Part of the Integral Homology

For any positive integer N, let $H^+(N) = H_1(X_0(N), \mathbb{Z})^+$ be the $+1$ eigen-submodule for the action of complex conjugation on the integral homology of $X_0(N)$. Then $H^+(N)$ is a module over the Hecke algebra $\mathbf{T}$. Let

$$F^+(N) = \operatorname{coker}\left(H^+(N) \times \operatorname{Hom}(H^+(N), \mathbb{Z}) \to \operatorname{Hom}(\mathbf{T}, \mathbb{Z})\right)$$

where the map sends (x, φ) to the homomorphism $t \mapsto \varphi(tx)$. Then $\#F^+(p) \in \{1, 2, 4\}$ for all primes $p < 389$, but $\#F^+(389) = 8$.

5.4 The Field Generated By Points of Small Prime Order On an Elliptic Curve

The prime 389 arises in a key way in the verification of condition 3 in [11].

References

[1] A. Agashe and W. A. Stein, Appendix to Joan-C. Lario and René Schoof: *Some computations with Hecke rings and deformation rings*, submitted.

[2] ———, *Visible evidence for the birch and swinnerton-dyer conjecture for modular abelian varieties of analytic rank* 0, In Preparation.

[3] ———, *Visibility of Shafarevich-Tate Groups of Abelian Varieties*, to appear in J. of Number Theory (2002).

[4] J. E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997.

[5] N. D. Elkies, *Elliptic and modular curves over finite fields and related computational issues*, Computational perspectives on number theory (Chicago, IL, 1995), Amer. Math. Soc., Providence, RI, 1998, pp. 21–76.

[6] E. V. Flynn, F. Leprévost, E. F. Schaefer, W. A. Stein, M. Stoll, and J. L. Wetherell, *Empirical evidence for the Birch and Swinnerton-Dyer conjectures for modular Jacobians of genus 2 curves*, Math. Comp. **70** (2001), no. 236, 1675–1697 (electronic).

[7] B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320.

[8] V. A. Kolyvagin, *Finiteness of $E(\mathbf{q})$ and $SH(E, \mathbf{q})$ for a subclass of Weil curves*, Izv. Akad. Nauk SSSR Ser. Mat. **52** (1988), no. 3, 522–540, 670–671.

[9] ———, *The Mordell-Weil and Shafarevich-Tate groups for Weil elliptic curves*, Izv. Akad. Nauk SSSR Ser. Mat. **52** (1988), no. 6, 1154–1180, 1327.

[10] W. J. McGraw and K. Ono, *Modular form Congruences and Selmer groups*, preprint (2002).

[11] L. Merel and W. A. Stein, *The field generated by the points of small prime order on an elliptic curve*, Internat. Math. Res. Notices (2001), no. 20, 1075–1082.

[12] J.-F. Mestre, *La méthode des graphes. Exemples et applications*, Proceedings of the international conference on class numbers and fundamental units of algebraic number fields (Katata) (1986), 217–242.

[13] K. A. Ribet, *Endomorphisms of semi-stable abelian varieties over number fields*, Ann. Math. (2) **101** (1975), 555–562.

[14] ———, *Torsion points on $J_0(N)$ and Galois representations*, Arithmetic theory of elliptic curves (Cetraro, 1997), Springer, Berlin, 1999, pp. 145–166.

[15] J-P. Serre, *A Course in Arithmetic*, Springer-Verlag, New York, 1973, Translated from the French, Graduate Texts in Mathematics, No. 7.

[16] G. Shimura, *On the factors of the jacobian variety of a modular function field*, J. Math. Soc. Japan **25** (1973), no. 3, 523–544.

[17] J. Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire Bourbaki, Vol. 9, Soc. Math. France, Paris, 1995, pp. Exp. No. 306, 415–440.

[18] D. Zagier, *Modular points, modular curves, modular surfaces and modular forms*, Workshop Bonn 1984 (Bonn, 1984), Springer, Berlin, 1985, pp. 225–248.