Component Groups of Quotients of $J_0(N)$

David Kohel[1] and William A. Stein[2]

[1] University of Sydney
kohel@maths.usyd.edu.au
http://www.maths.usyd.edu.au:8000/u/kohel/
[2] University of California at Berkeley,
was@math.berkeley.edu
http://shimura.math.berkeley.edu/~was

Abstract. Let f be a newform of weight 2 on $\Gamma_0(N)$, and let A_f be the corresponding optimal abelian variety quotient of $J_0(N)$. We describe an algorithm to compute the order of the component group of A_f at primes p that exactly divide N. We give a table of orders of component groups for all f of level $N \leq 127$ and five examples in which the component group is very large, as predicted by the Birch and Swinnerton-Dyer conjecture.

1 Introduction

Let $X_0(N)$ be the Riemann surface obtained by compactifying the quotient of the upper half-plane by the action of $\Gamma_0(N)$. Then $X_0(N)$ has a canonical structure of algebraic curve over $\mathbf{Q}$; denote its Jacobian by $J_0(N)$. It is equipped with an action of a commutative ring $\mathbf{T} = \mathbf{Z}[\ldots T_n \ldots]$ of Hecke operators. For more details on modular curves, Hecke operators, and modular forms see, e.g., [8].

Now suppose that $f = \sum_{n=1}^{\infty} a_n q^n$ is a modular newform of weight 2 for the congruence subgroup $\Gamma_0(N)$. The Hecke operators also act on f by $T_n(f) = a_n f$. The eigenvalues a_n generate an order $R_f = \mathbf{Z}[\ldots a_n \ldots]$ in a number field K_f. The kernel I_f of the map $\mathbf{T} \to R_f$ sending T_n to a_n is a prime ideal. Following Shimura [15], we associate to f the quotient $A_f = J_0(N)/I_f J_0(N)$ of $J_0(N)$. Then A_f is an abelian variety over $\mathbf{Q}$ of dimension $[K_f : \mathbf{Q}]$, with bad reduction exactly at the primes dividing N.

One-dimensional quotients of $J_0(N)$ have been intensely studied in recent years, both computationally and theoretically. The original conjectures of Birch and Swinnerton-Dyer [1, 2], for elliptic curves over $\mathbf{Q}$, were greatly influenced by computations. The scale of these computations was extended and systematized by Cremona in [6].

In another direction, Wiles [20] and Taylor-Wiles [18] proved a special case of the conjecture of Shimura-Taniyama, which asserts that every elliptic curve over $\mathbf{Q}$ is a quotient of some $J_0(N)$; this allowed them to establish Fermat's Last Theorem. The full Shimura-Taniyama conjecture was later proved by Breuil, Conrad, Diamond, and Taylor in [4]. This illustrates the central role played by quotients of $J_0(N)$.

2 Component Groups of A_f

The Néron model $\mathcal{A}/\mathbf{Z}$ of an abelian variety $A/\mathbf{Q}$ is by definition a smooth commutative group scheme over $\mathbf{Z}$ with generic fiber A such that for any smooth scheme S over $\mathbf{Z}$, the restriction map

$$\mathrm{Hom}_{\mathbf{Z}}(S, \mathcal{A}) \to \mathrm{Hom}_{\mathbf{Q}}(S_{\mathbf{Q}}, A)$$

is a bijection. For more details, including a proof of existence, see, e.g., [5].

Suppose that A_f is a quotient of $J_0(N)$ corresponding to a newform f on $\Gamma_0(N)$, and let $\mathcal{A}_f$ be the Néron model of A_f. For any prime divisor p of N, the closed fiber $\mathcal{A}_{f/\mathbf{F}_p}$ is a group scheme over $\mathbf{F}_p$, which need not be connected. Denote the connected component of the identity by $\mathcal{A}^{\circ}_{f/\mathbf{F}_p}$. There is an exact sequence

$$0 \to \mathcal{A}^{\circ}_{f/\mathbf{F}_p} \to \mathcal{A}_{f/\mathbf{F}_p} \to \Phi_{A_f,p} \to 0$$

with $\Phi_{A_f,p}$ a finite étale group scheme over $\mathbf{F}_p$ called the *component group* of A_f at p.

The category of finite étale group schemes over $\mathbf{F}_p$ is equivalent to the category of finite groups equipped with an action of $\mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$ (see, e.g., [19, §6.4]). The *order* of an étale group scheme $G/\mathbf{F}_p$ is defined to be the order of the group $G(\overline{\mathbf{F}}_p)$. In this paper we describe an algorithm for computing the order of $\Phi_{A_f,p}$, when p exactly divides N.

3 The Algorithm

Let $J = J_0(N)$, fix a newform f of weight-two for $\Gamma_0(N)$, and let A_f be the corresponding quotient of J. Because J is the Jacobian of a curve, it is canonically isomorphic to its dual, so the projection $J \to A_f$ induces a polarization $A_f^{\vee} \to A_f$, where $A_f^{\vee}$ denotes the abelian variety dual of A_f. We define the *modular degree* δ_{A_f} of A_f to be the positive square root of the degree of this polarization. This agrees with the usual notion of modular degree when A_f is an elliptic curve.

A *torus* T over a field k is a group scheme whose base extension to the separable closure k_s of k is a finite product of copies of $\mathbf{G}_m$. Every commutative algebraic group over k admits a unique maximal subtorus, defined over k, whose formation commutes with base extension (see IX §2.1 of [9]). The *character group* of a torus T is the group $\mathcal{X} = \mathrm{Hom}_{k_s}(T, \mathbf{G}_m)$ which is a free abelian group of finite rank together with an action of $\mathrm{Gal}(k_s/k)$ (see, e.g., [19, §7.3]).

We apply this construction to our setting as follows. The closed fiber of the Néron model of J at p is a group scheme over $\mathbf{F}_p$, whose maximal torus we denote by $T_{J,p}$. We define $\mathcal{X}_{J,p}$ to be the character group of $T_{J,p}$. Then $\mathcal{X}_{J,p}$ is a free abelian group equipped with an action of both $\mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$ and the Hecke algebra $\mathbf{T}$ (see, e.g., [14]). Moreover, there exists a bilinear pairing

$$\langle\, , \,\rangle : \mathcal{X}_{J,p} \times \mathcal{X}_{J,p} \to \mathbf{Z}$$

called the *monodromy pairing* such that

$$\Phi_{J,p} \cong \mathrm{coker}(\mathcal{X}_{J,p} \to \mathrm{Hom}(\mathcal{X}_{J,p}, \mathbf{Z})).$$

Let $\mathcal{X}_{J,p}[I_f]$ be the intersection of all kernels $\ker(t)$ for t in I_f, and let

$$\alpha_f : \mathcal{X}_{J,p} \to \mathrm{Hom}(\mathcal{X}_{J,p}[I_f], \mathbf{Z})$$

be the map induced by the monodromy pairing. The following theorem of the second author [16], provides the basis for the computation of orders of component groups.

Theorem 1. *With the notation as above, we have the equality*

$$\#\Phi_{A_f,p} = \frac{\#\mathrm{coker}(\alpha_f) \cdot \delta_{A_f}}{\#(\alpha_f(\mathcal{X}_{J,p})/\alpha_f(\mathcal{X}_{J,p}[I_f]))} .$$

3.1 Computing the modular degree $\boldsymbol{\delta_{A,f}}$

Using modular symbols (see, e.g., [6]), we first compute the homology group $H_1(X_0(N), \mathbf{Q}; \text{cusps})$. Using lattice reduction, we compute the $\mathbf{Z}$-submodule $H_1(X_0(N), \mathbf{Z}; \text{cusps})$ generated by all Manin symbols (c, d). Then $H_1(X_0(N), \mathbf{Z})$ is the *integer* kernel of the boundary map.

The Hecke ring $\mathbf{T}$ acts on $H_1(X_0(N), \mathbf{Z})$ and also on the linear dual $\mathrm{Hom}(H_1(X_0(N), \mathbf{Z}), \mathbf{Z})$, where $t \in \mathbf{T}$ acts on $\varphi \in \mathrm{Hom}(H_1(X_0(N), \mathbf{Z}), \mathbf{Z})$ by $(t.\varphi)(x) = \varphi(tx)$. We have a natural restriction map

$$r_f : \mathrm{Hom}(H_1(X_0(N), \mathbf{Z}), \mathbf{Z})[I_f] \to \mathrm{Hom}(H_1(X_0(N), \mathbf{Z})[I_f], \mathbf{Z}).$$

Proposition 1. *The cokernel of r_f is isomorphic to the kernel of the polarization $A_f^\vee \to A_f$ induced by the map $J_0(N) \to A_f$.*

Thus the order of the cokernel of r_f is the square of the modular degree δ_f. We pause to note that the degree of any polarization is a square; see, e.g., [13, Thm. 13.3].

Proof. Let $S = S_2(\Gamma_0(N), \mathbf{C})$ be the complex vector space of weight-two modular forms of level N, and set $H = H_1(X_0(N), Z)$. The integration pairing $S \times H \to \mathbf{C}$ induces a natural map

$$\Phi_f : H \to \mathrm{Hom}(S[I_f], \mathbf{C}).$$

Using the classical Abel-Jacobi theorem, we deduce the following commutative diagram, which has exact columns, but whose rows are not exact.

$$\begin{tikzcd}
0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] \\
H[I_f] \arrow[r] \arrow[d] & H \arrow[r] \arrow[d] & \Phi_f(H) \arrow[d] \\
\mathrm{Hom}(S, \mathbf{C})[I_f] \arrow[r] \arrow[d] & \mathrm{Hom}(S, \mathbf{C}) \arrow[r] \arrow[d] & \mathrm{Hom}(S[I_f], \mathbf{C}) \arrow[d] \\
A_f^\vee(\mathbf{C}) \arrow[r] \arrow[d] \arrow[rr, bend right=60] & J_0(N)(\mathbf{C}) \arrow[r] \arrow[d] & A_f(\mathbf{C}) \arrow[d] \\
0 & 0 & 0
\end{tikzcd}$$

By the snake lemma, the kernel of $A_f^\vee(\mathbf{C}) \to A_f(\mathbf{C})$ is isomorphic to the cokernel of the map $H[I_f] \to \Phi_f(H)$. Since

$$\mathrm{Hom}(H/\ker(\Phi_f), \mathbf{Z}) \cong \mathrm{Hom}(H, \mathbf{Z})[I_f],$$

the $\mathrm{Hom}(-, \mathbf{Z})$ dual of the map $H[I_f] \to \Phi_f(H) = H/\ker(\Phi_f)$ is r_f, which proves the proposition.

3.2 Computing the character group $\mathcal{X}_{J,p}$

Let $N = Mp$, where M and p are coprime. If M is small, then the algorithm of Mestre and Oesterlé [12] can be used to compute $\mathcal{X}_{J,p}$. This algorithm constructs the graph of isogenies between $\overline{\mathbf{F}}_p$-isomorphism classes of pairs consisting of a supersingular elliptic curve and a cyclic M-torsion subgroup. In particular, the method is elementary to apply when $X_0(M)$ has genus 0.

In general, the above category of "enhanced" supersingular elliptic curves can be replaced by one of left (or right) ideals of a quaternion order $\mathcal{O}$ of level M in the quaternion algebra over $\mathbf{Q}$ ramified at p. This gives an equivalent category, in which the computation of homomorphisms is efficient. The character group $\mathcal{X}_{J,p}$ is known by Deligne-Rapoport [7] to be canonically isomorphic to the degree zero subgroup $\mathcal{X}(\mathcal{O})$ of the free abelian "divisor group" on the isomorphism classes of enhanced supersingular elliptic curves and of quaternion ideals. Moreover, this isomorphism is compatible with the operation of Hecke operators, which are effectively computable in $\mathcal{X}(\mathcal{O})$ in terms of ideal homomorphisms.

The inner product of two classes in this setting is defined to be the number of isomorphisms between any two representatives. The linear extension to $\mathcal{X}(\mathcal{O})$ gives an inner product which agrees, under the isomorphism, with the monodromy pairing on $\mathcal{X}_{J,p}$. This gives, in particular, an isomorphism $\Phi_{J,p} \cong \mathrm{coker}(\mathcal{X}(\mathcal{O}) \to \mathrm{Hom}(\mathcal{X}(\mathcal{O}), \mathbf{Z}))$, and an effective means of computing $\#\mathrm{coker}(\alpha_f)$ and $\#(\alpha_f(\mathcal{X}_{J,p})/\alpha_f(\mathcal{X}_{J,p}[I_f]))$.

The arithmetic of quaternions has been implemented in Magma [11] by the first author. Additional details and the application to Shimura curves, generalizing $X_0(N)$, can be found in Kohel [10].

3.3 The Galois action on $\Phi_{A_f,p}$

To determine the Galois action on $\Phi_{A_f,p}$, we need only know the action of the Frobenius automorphism Frob_p. However, Frob_p acts on $\Phi_{A_f,p}$ in the same way as $-W_p$, where W_p is the pth Atkin-Lehner involution, which can be computed using modular symbols. Since f is an eigenform, the involution W_p acts as either $+1$ or -1 on $\Phi_{A_f,p}$. Moreover, the operator W_p is determined by an involution on the set of quaternion ideals, so it can be determined explicitly on the character group.

4 Tables

The main computational results of this work are presented below in two tables. The relevant algorithms have been implemented in Magma and will be made part of a future release. They can also be obtained from the second author.

4.1 Component groups at low level

The first table gives the component groups of the quotients A_f of $J_0(N)$ for $N \leq 127$. The column labeled d contains the dimensions of the A_f, and the column labeled $\#\Phi_{A_f,p}$ contains a list of the orders of the component groups of A_f, one for each divisor p of N, ordered by increasing p. An entry of "?" indicates that $p^2 \mid N$, so our algorithm does not apply. A component group order is starred if the $\mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$-action is nontrivial. More data along these lines can be obtained from the second author.

4.2 Examples of large component groups

Let Ω_{A_f} be the real period of A_f, as defined by J. Tate in [17]. The second author computed the rational numbers $L(A_f, 1)/\Omega_{A_f}$ for every newform f of level $N \leq 1500$. The five largest prime divisors occur in the ratios given in the second table. The Birch and Swinnerton-Dyer conjecture predicts that the large prime divisor of the numerator of each special value must divide the order either of some component group $\Phi_{A_f,p}$ or of the Shafarevich-Tate group of A_f. In each instance $\Phi_{A_f,2}$ is divisible by the large prime divisor, as predicted.

5 Further directions

Further considerations are needed to compute the *group* structure of $\Phi_{A_f,p}$. However, since the action of Frobenius is known, computing the group structure of $\Phi_{A_f,p}$ suffices to determine its structure as a group scheme.

Our methods say nothing about the component group at primes whose *square* divides the level. The free abelian group on classes of nonmaximal orders of index p at a ramified prime gives a well-defined divisor group. Do the resulting Hecke modules determine the component groups for quotients of level p^2M?

Is it possible to define quantities as in Theorem 1 even when the weight of f is *greater than* 2? If so, how are the resulting quantities related to the Bloch-Kato Tamagawa numbers (see [3]) of the higher weight motive attached to f?

Component groups at low level

N	d	$\#\Phi_{A_f,p}$	N	d	$\#\Phi_{A_f,p}$	N	d	$\#\Phi_{A_f,p}$	N	d	$\#\Phi_{A_f,p}$	N	d	$\#\Phi_{A_f,p}$
11	1	5		3	13	76	1	?,1*	96	1	?,2		3	7
14	1	6*,3	54	1	3*,?	77	1	2*,1*		1	?,2*	114	1	2*,5*,1
15	1	4*,4		1	3,?		1	3*,2	97	3	1*		1	20,3*,1*
17	1	4	55	1	2,2*		1	6,3*		4	8		1	6,3,1
19	1	3		2	14*,2		2	2,2*	98	1	2*,?	115	1	5*,1
20	1	?,2*	56	1	?,1	78	1	16*,5*,1		2	14,?		2	4*,1*
21	1	4,2*		1	?,1*	79	1	1*	99	1	?,1*		4	32,4*
23	2	11	57	1	2*,1*		5	13		1	?,1	116	1	?,1*
24	1	?,2*		1	2,2*	80	1	?,2		1	?,1*		1	?,2*
26	1	3*,3		1	10,1*		1	?,2*		1	?,1*		1	?,1*
	1	7,1*	58	1	2*,1*	81	2	?	100	1	?,?	117	1	?,1
27	1	?		1	10,1*	82	1	2*,1*	101	1	1*		2	?,3
29	2	7	59	5	29		2	28,1*		7	25		2	?,1*
30	1	4*,3,1*	61	1	1*	83	1	1*	102	1	2*,2*,1*	118	1	2*,1*
31	2	5		3	5		6	41		1	6*,6,1*		1	19*,1
32	1	?	62	1	4,1*	84	1	?,1*,2*		1	8,4,1		1	10,1*
33	1	6*,2		2	66*,3		1	?,3,2	103	2	1*		1	1,1*
34	1	6,1*	63	1	?,1*	85	1	2*,1		6	17	119	4	9,3*
35	1	3*,3		2	?,3		2	2*,1*	104	1	?,1*		5	48*,8
	2	8,4*	64	1	?		2	6,1*		2	?,2	120	1	?,1,1*
36	1	?,?	65	1	1*,1*	86	2	21*,3	105	1	1,1,1		1	?,2,1
37	1	1*		2	3*,3		2	55,1*		2	10*,2*,2	121	1	?
	1	3		2	7,1*	87	2	5,1*	106	1	4*,1*		1	?
38	1	9*,3	66	1	2*,3,1*		3	92*,4		1	5*,1		1	?
	1	5,1*		1	4,1*,1*	88	1	?,1*		1	24,1*		1	?
39	1	2*,2		1	10,5,1		2	?,2*		1	3,1*	122	1	4*,1*
	2	14,2*	67	1	1	89	1	1*	107	2	1*		2	39*,3
40	1	?,2		2	1*		1	2		7	53		3	248,1*
41	3	10		2	11		5	11	108	1	?,?	123	1	1*,1*
42	1	8,2*,1*	68	2	?,2*	90	1	2*,?,3	109	1	1		1	5,1
43	1	1*	69	1	2,1*		1	6,?,1*		3	1*		2	7,1*
	2	7		2	22*,2		1	4,?,1		4	9		3	184*,4
44	1	?,1*	70	1	4,2*,1*	91	1	1*,1*	110	1	7*,1*,3	124	1	?,1*
45	1	?,1*	71	3	5		1	1,1		1	3,1*,1*		1	?,1
46	1	10*,1		3	7		2	7,1*		1	5,5,1	125	2	?
47	4	23	72	1	?,?		3	4*,8		2	16*,3,1*		2	?
48	1	?,2	73	1	2	92	1	?,1*	111	3	10*,2		4	?
49	1	?		2	1*		1	?,1		4	266,2*	126	1	8*,?,1*
50	1	1*,?		2	3	93	2	4*,1*	112	1	?,1*		1	2,?,1
	1	5,?	74	2	9*,3		3	64,2*		1	?,1	127	3	1*
51	1	3,1*		2	95,1*	94	1	2,1*		1	?,1*		7	21
	2	16*,4	75	1	1*,?		2	94*,1	113	1	2			
52	1	?,2*		1	1,?	95	3	10,2*		2	2			
53	1	1*		1	5,?		4	54*,6		3	1*			

Large $L(A_f,1)/\Omega_{A_f}$

N	dim	$L(A_f,1)/\Omega_{A_f}$	$\#\Phi_{A_f,p}$
$1154 = 2{\cdot}577$	20	$2^?{\cdot}85495047371/17^2$	$2^?{\cdot}17^2{\cdot}85495047371, 2^?$
$1238 = 2{\cdot}619$	19	$2^?{\cdot}7553329019/5{\cdot}31$	$2^?{\cdot}5{\cdot}31{\cdot}7553329019, 2^?$
$1322 = 2{\cdot}661$	21	$2^?{\cdot}57851840099/331$	$2^?{\cdot}331{\cdot}57851840099, 2^?$
$1382 = 2{\cdot}691$	20	$2^?{\cdot}37{\cdot}1864449649/173$	$2^?{\cdot}37{\cdot}173{\cdot}1864449649, 2^?$
$1478 = 2{\cdot}739$	20	$2^?{\cdot}7{\cdot}29{\cdot}1183045463/5{\cdot}37$	$2^?{\cdot}5{\cdot}7{\cdot}29{\cdot}37{\cdot}1183045463, 2^?$

References

1. B. J. Birch, and H. P. F. Swinnerton-Dyer, *Notes on elliptic curves, I*, J. Reine Angew. Math. **212** (1963), 7–25.
2. B. J. Birch and H. P. F. Swinnerton-Dyer, *Notes on elliptic curves, II*, J. Reine Angew. Math. **218** (1965), 79–108.
3. S. Bloch and K. Kato, *L-functions and Tamagawa numbers of motives*, The Grothendieck Festschrift, Vol. I, Birkhäuser Boston, Boston, MA, 1990, 333–400.
4. C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$, in preparation.
5. S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, Springer-Verlag, Berlin, 1990.
6. J. E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997.
7. P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, In P. Deligne and W. Kuyk, eds., *Modular functions of one variable, Vol. II*, Lecture Notes in Math., **349**, Springer, Berlin, 1973, 143–316.
8. F. Diamond and J. Im, *Modular forms and modular curves*, In V. K. Murty, ed., *Seminar on Fermat's Last Theorem*, Amer. Math. Soc., Providence, RI, 1995, 39–133.
9. A. Grothendieck, *Séminaire de géométrie algébrique du Bois-Marie 1967–1969 (SGA 7 I)*, Lecture Notes in Mathematics, **288**, Springer-Verlag, Berlin-New York, 1972
10. D. Kohel, *Hecke module structure of quaternions*, In K. Miyake, ed., *Class Field Theory – Its Centenary and Prospect*, The Advanced Studies in Pure Mathematics Series, Math Soc. Japan, to appear.
11. W. Bosma, J. Cannon, and C. Playoust. *The Magma algebra system I: The user language*, J. Symb. Comp., **24** (1997), no. 3-4, 235–265.
12. J.-F. Mestre, *La méthode des graphes. Exemples et applications*, In *Proceedings of the international conference on class numbers and fundamental units of algebraic number fields*, Nagoya University, Nagoya, 1986, 217–242.
13. J.S. Milne, *Abelian Varieties*, In G. Cornell and J. Silverman, eds., *Arithmetic geometry*, Springer, New York, 1986, 103–150,
14. K. A. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), no. 2, 431–476.
15. G. Shimura, *On the factors of the jacobian variety of a modular function field*, J. Math. Soc. Japan **25** (1973), no. 3, 523–544.
16. W. A. Stein, *Explicit approaches to modular abelian varieties*, Ph.D. thesis, University of California, Berkeley, 2000.
17. J. Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire Bourbaki, Vol. 9, Soc. Math. France, Paris, 1995, Exp. No. 306, 415–440.

18. R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. **141** (1995), no. 3, 553–572.
19. W. C. Waterhouse, *Introduction to affine group schemes*, Graduate Texts in Mathematics, **66**, Springer-Verlag, New York-Berlin, 1979
20. A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. **141** (1995), no. 3, 443–551.