Modular abelian varieties
of odd modular degree

Soroosh Yazdani

Modular abelian varieties
of odd modular degree

Soroosh Yazdani

We study modular abelian varieties with odd congruence number by examining the cuspidal subgroup of $J_0(N)$. We show that the conductor of such abelian varieties must be of a special type. For example, if N is the conductor of an absolutely simple modular abelian variety with odd congruence number, then N has at most two prime divisors, and if N is odd, then $N = p^\alpha$ or $N = pq$ for some primes p and q. In the second half of the paper, we focus on modular elliptic curves with odd modular degree. Our results, combined with the work of Agashe, Ribet, and Stein for elliptic curves to have odd modular degree. In the process we prove Watkins' conjecture for elliptic curves with odd modular degree and a nontrivial rational torsion point.

Let $E/\mathbb{Q}$ be an elliptic curve over the rational numbers. From [Wiles 1995; Taylor and Wiles 1995], we know that E is modular (see [Breuil et al. 2001]), which implies that there is a surjective map $\pi : X_0(N) \to E$ defined over the rationals. As such, we have a new invariant attached to the elliptic curve, namely the minimal degree of π, which we call the *modular degree* of E. This invariant is related to many other invariants of the elliptic curve. For instance, this number is closely related to the congruences between E and other modular forms (see Section 1A and [Agashe et al. 2008]). Also, we know that finding a good bound on the degree of π in terms of N is equivalent to the ABC conjecture (see [Murty 1999; Frey 1997]).

After calculating the modular degree of various elliptic curves, Watkins conjectured that 2^r divides the modular degree of the elliptic curve E, where r is the rank of $E(\mathbb{Q})$ (see [Watkins 2002]). In the particular case when the modular degree of E is odd, Watkins' conjecture implies $E(\mathbb{Q})$ is finite. Searching through Cremona, Stein, and Watkins' databases [Stein and Watkins 2002; Cremona] for elliptic curves of odd modular degree, Calegari and Emerton [2009] observed that all such elliptic curves have bad reduction at no more than two primes. By studying the Atkin–Lehner involution on elliptic curves E having odd modular degree, they

demonstrated that such curves have an even analytic rank and that there are at most two odd primes dividing their conductor (see Section 2A). Dummigan [2006] has provided a heuristic explanation for Watkins' conjecture. His method uses the Selmer group of the symmetric square of E and its relationship to congruences between modular forms.

The goal of this paper is to extend the results of Calegari and Emerton to modular abelian varieties having odd modular exponents and odd congruence number (see Section 1A for definition). We find the necessary conditions for a modular abelian variety to have odd congruence number. Specifically in Theorem 2.15 we show that if a modular abelian variety with conductor N has odd congruence number, then $N = 2p, 4p^a, 8p^a, pq$ where p and q are odd primes, or N is a power of a prime. In Section 3 we study elliptic curves having odd congruence number. Recall the result of Agashe, Ribet, and Stein [Agashe et al. 2008] that elliptic curves with semistable reduction at 2 have odd congruence number if and only if they have odd modular degree (see Theorem 1.1).[1] We find more stringent conditions that elliptic curves with odd congruence number need to satisfy. Specifically in Theorem 3.8 we show that if an elliptic curve E with conductor N has odd congruence number, then if it has a trivial torsion structure then N is prime and E has an even analytic rank, otherwise N has at most two prime divisors and has rank 0. Furthermore, we find families of elliptic curves that any elliptic curve with odd congruence number and a nontrivial torsion point must belong to one of these families (see Theorem 3.8). We expect that the elliptic curves in these families have odd modular degrees, although to prove this we need a better understanding of the rational torsion points of $J_0(N)$.

We now give a quick overview. In Section 1, we review some definitions and results needed in the rest of the paper. Specifically, in Section 1B we recall how to calculate the rational cuspidal subgroup of $J_0(N)$, and in Section 1C we study the action of the Hecke algebra and Atkin–Lehner involutions on this subgroup. In Section 2, we study modular abelian varieties with odd congruence number, and show that all such abelian varieties have at most two primes of bad reduction. A key component of this argument is that if A is a modular abelian variety having odd congruence number and non-prime-power conductor, A must have a rational 2-torsion point (Theorem 2.1). We also show that if A has odd congruence number and a rational 2-torsion point, then all the new rational 2-torsion points of $J_0(N)$ map injectively to A (see Section 2C). We use this fact and our analysis of the cuspidal subgroup to show that if A has odd congruence number and is semistable away from 2, then it has at most two primes of bad reduction (Theorem 2.12) and the primes dividing the conductor must satisfy certain congruences (Theorem 2.15). The other useful result is that if $p^2 | N$ for some odd prime N, then A must have a

---

[1]In fact, by searching through Cremona's table of elliptic curves, it seems that an elliptic curve has odd congruence number if and only if it has odd modular degree.

complex multiplication or an inner twist (Proposition 2.10). In Section 3 we apply our results to elliptic curves. Theorem 2.15 gives us conditions that the conductor of an elliptic curve with odd congruence number must satisfy. In each subsection of Section 3 we study one of these cases, get more stringent conditions on the conductor, and show that in almost all cases the rank of such elliptic curves is zero (Theorem 3.8).

1. Preliminaries

Let N be a positive integer and $X_0(N)$ be the moduli space of generalized elliptic curves with a cyclic subgroup of order N. Let $\mathscr{C}_N \subset X_0(N)$ be the set of cusps of $X_0(N)$, that is, $\mathscr{C}_N = \pi^{-1}(\infty)$, where $\pi : X_0(N) \to X_0(1)$ is the natural degeneracy map, and ∞ is the unique cusp on $X_0(1)$. All such cusps can be represented as rational numbers $a/b \in \mathbb{H}$, with a and b positive coprime integers and $b|N$. Furthermore, there is a unique representative for any cusp with $a \le (b, N/b)$. Under this representation, $\infty = 1/N$. For any divisor r of N with $\gcd(r, N/r) = 1$, we can define the Atkin–Lehner involution $w_r : X_0(N) \to X_0(N)$ by sending (E, D) to $(E/D[r], (E[r] + D)/D[r])$[2]. We usually abuse notation by letting $w_{\bar{r}} = w_r$ whenever $\bar{r} = \prod_{l|r} l$ (for example, $w_4 = w_2$ on $X_0(4N)$).

Let $S(N)$ be the space of weight two cuspforms on $\Gamma_0(N)$. Let $\mathbb{T}$ denote the $\mathbb{Z}$-algebra of the Hecke operators acting on $S(N)$. As usual, we denote $J_0(N) = \mathrm{Jac}(X_0(N))$. Then $\mathbb{T}$ acts faithfully on $J_0(N)$ by Picard functoriality. We also have the standard Albanese embedding $i : X_0(N) \to J_0(N)$ via $i(z) = (z) - (\infty)$. Note that for any map $w : X_0(N) \to X_0(N)$ we have the induced map

$$w_* : J_0(N) \to J_0(N),$$
$$\sum(z) \mapsto \sum(w(z)).$$

1A. Congruence numbers. Recall that attached to any newform $f \in S(N)$ we have a modular abelian variety A_f. Specifically, let I_f be the kernel of $\mathbb{T} \to \mathbb{C}$ induced by f. Then we have $A_f = J_0(N)/I_f$, which we refer to as the *optimal quotient* attached to f. Conversely, if A is a simple quotient of $J_0(N)$ that is stable under the action of $\mathbb{T}$ and the Atkin–Lehner involutions, then we can find a modular eigenform $f \in S(N)$ such that A is isogenous to A_f. In this case, we say that f is attached to A. Furthermore all modular forms attached to A are Galois conjugate to f. Let $\phi : J_0(N) \to A$ be a surjective morphism. Then the dual morphism is $\phi^\vee : A^\vee \to J_0(N)^\vee$. Since $J_0(N)$ is self-dual, we can compose these two morphisms to get

$$\psi : A^\vee \to A.$$

---

[2]As usual, $G[r]$ is the set of r-torsion points of the group G.

Following [Agashe et al. 2008], we define the *modular number* to be the order of
$\ker(\psi)$, and the *modular exponent* to be its exponent, denoted by $\widetilde{n}_A$. If A is an
elliptic curve, then $\widetilde{n}_A$ equals the modular degree of A. In fact, in the case of elliptic
curves we get that $\ker(\psi) = A[\deg(\pi)]$, where $\pi : X_0(N) \to A$ (see Lemma 2.2).

Now let $\phi : J_0(N) \to A$ be any optimal modular abelian quotient. Let $B = \ker(\phi)$,
which is an abelian variety since A is an optimal quotient. Let $\mathbb{T}_A$ be the $\mathbb{Z}$-algebra
of the Hecke operators acting on A. Similarly, let $\mathbb{T}_B$ be the $\mathbb{Z}$-algebra of the
Hecke operators acting on B. There is an injective map $\mathbb{T} \to \mathbb{T}_A \oplus \mathbb{T}_B$ with a finite
index, given by the restriction map. The order of the cokernel of $\mathbb{T} \to \mathbb{T}_A \oplus \mathbb{T}_B$
is the *congruence number* of A. The exponent of this cokernel is the *congruence
exponent* of A, which is denoted by $\widetilde{r}_A$ (see [Agashe et al. 2008, Lemma 4.3]).
Let $\mathfrak{m} \subset \mathbb{T}$ be a maximal ideal of $\mathbb{T}$. Then $A[\mathfrak{m}] \neq 0$ (resp. $B[\mathfrak{m}] \neq 0$) if and
only if the image of $\mathfrak{m}$ in $\mathbb{T}_A$ (resp. $\mathbb{T}_B$) is a proper maximal ideal. If $A[\mathfrak{m}]$ and
$B[\mathfrak{m}]$ are both nontrivial, then by tensoring $\mathbb{T} \to \mathbb{T}_A \oplus \mathbb{T}_B$ by $\mathbb{T}/\mathfrak{m}$, we see that the
cokernel is a nontrivial vector space over $\mathbb{T}/\mathfrak{m}$, which means that the characteristic
of $\mathbb{T}/\mathfrak{m}$ divides the congruence exponent of A. On the other hand, if $A[\mathfrak{m}] \neq 0$,
then $A^\vee[\mathfrak{m}] \neq 0$, and if $A^\vee[\mathfrak{m}] \cap B[\mathfrak{m}] \neq 0$, the characteristic of $\mathbb{T}/\mathfrak{m}$ divides the
modular exponent.

In [Agashe et al. 2008], the relationship between the modular exponent and the
congruence exponent was studied, and the following was proved.

Theorem 1.1. *If $f \in S(N)$ is a newform, then $\widetilde{n}_{A_f} | \widetilde{r}_{A_f}$. If, moreover, $p^2 \nmid N$, then*
$\operatorname{ord}_p(\widetilde{n}_{A_f}) = \operatorname{ord}_p(\widetilde{r}_{A_f})$.

In particular, if f is a newform of level N and $4 \nmid N$, then the modular exponent
of A_f is odd if and only if its congruence exponent is odd.

1B. *Cuspidal subgroup.* The cuspidal subgroup of $J_0(N)$ is the subgroup gener-
ated by the cusps of $X_0(N)$. The goal of this section is to understand the rational
points of the cuspidal subgroup of $J_0(N)$, denoted by C_N. This problem was
studied for N a power of a prime in [Ling 1997] and for N the product of the two
primes in [Chua and Ling 1997]. Set

$$P_d = \frac{1}{\gcd(d, N/d)} \sum_{i=1}^{\gcd(d, N/d)} (id/N)^3.$$

Proposition 1.2 [Ling 1997]. *The rational cuspidal subgroup $C_N \subset J_0(N)$ is gen-
erated by the elements $\phi(\gcd(d, N/d))(P_d - P_1)$.*

Here and in Proposition 1.4, ϕ denotes the Euler totient function. However,

---

[3]Our notation is slightly different from [Ling 1997; Chua and Ling 1997]. Specifically their P_d
is $\gcd(d, N/d)$ times our P_d.

outside this section, ϕ is reserved for the map $\phi : J_0(N) \to A$, and whenever results from this section are used, we will have $\phi(\gcd(d, N/d)) = 1$.

We will calculate the order of certain elements in C_N. Recall the Dedekind eta function, defined as

$$\eta(\tau) = q^{1/24} \prod_{n=1}^{\infty} (1 - q^n), \quad \text{with } q = e^{2\pi i \tau}.$$

Let $\eta(M\tau) = \eta_M(\tau)$. We use η_M to construct functions with divisors supported on the cusps. In particular, for $M|N$, η_M has a zero of order

$$\frac{1}{24} \frac{N d'^2}{dt M}, \tag{1}$$

at the cusp of $X_0(N)$ corresponding to $x/d \in \mathbb{H}$, where $d' = \gcd(d, M)$ and $t = \gcd(d, N/d)$; see, for example, [Ogg 1974].

Proposition 1.3 [Ligozat 1975]. *Let $\boldsymbol{r} = (r_\delta)$ be a collection of rational numbers $r_\delta \in \mathbb{Q}$ indexed by all the positive divisors of $\delta|N$. Then the function $g_{\boldsymbol{r}} = \prod_{\delta|N} \eta_\delta^{r_\delta}$ is a modular function on $X_0(N)$ if and only if the following conditions are satisfied:*

(1) *All the rational numbers r_δ are rational integers.*

(2) $\sum_{\delta|N} r_\delta \delta \equiv 0 \pmod{24}$.

(3) $\sum_{\delta|N} r_\delta N/\delta \equiv 0 \pmod{24}$.

(4) $\sum_{\delta|N} r_\delta = 0$.

(5) $\prod_{\delta|N} \delta^{r_\delta}$ *is a square of a rational number.*

We also know that the lattice of divisors linearly equivalent to zero supported on the cusps is generated by the divisors of $g_{\boldsymbol{r}}$ that are modular functions. Let $N = \prod_{i=1}^{k} p_i^{s_i}$ be the prime factorization of N, and let V be the rational vector space spanned by P_d for $d|N$. We can represent this vector space as the tensor product of the vector spaces V_{p_i}, where V_{p_i} is the $(s_i + 1)$-dimensional space generated by $P_1, P_{p_i}, \ldots, P_{p_i^{s_i}}$. (The isomorphism between V and the tensor product $\bigotimes_i V_{p_i}$ is the natural one sending $P_{\prod p_i^{\alpha_i}}$ to $P_{p_1^{\alpha_1}} \otimes \cdots \otimes P_{p_k^{\alpha_k}}$.) Similarly, let W be the rational vector space of functions $g_{\boldsymbol{r}}$ (as defined in Proposition 1.3) under multiplication. Then we have $W \simeq \bigotimes W_{p_i}$ where W_{p_i} is the $(s_i + 1)$-dimensional vector space generated by $\eta_1, \eta_{p_i}, \ldots, \eta_{p_i^{s_i}}$. We have an isomorphism $\Lambda : V \to W$ where $\Lambda^{-1}(g)$ is the divisor attached to g. We can verify that this isomorphism can be written very explicitly as

$$24 \Lambda_{p_1} \otimes \cdots \otimes \Lambda_{p_k},$$

where $\Lambda_{p_i} : V_{p_i} \to W_{p_i}$ is expressed in the basis above as the tridiagonal matrix

$$\Lambda_{p_i} = \frac{1}{(p_i^2-1)\phi(p_i^{s_i})}\begin{pmatrix} p_i(p_i-1) & -p_i & & & & \\ -(p_i-1) & p_i^2+1 & -p_i & & & \\ & -p_i & p_i^2+1 & -p_i & & \\ & & \ddots & \ddots & \ddots & \\ & & & -p_i & p_i^2+1 & -(p_i-1) \\ & & & & -p_i & p_i(p_i-1) \end{pmatrix}.$$

When $f \in W$ is a modular function, $\Lambda^{-1}(f)$ is linearly equivalent to zero. Therefore, by combining Proposition 1.3 and the isomorphism above we get:

Proposition 1.4. *An element $v \in \bigotimes V_{p_i} = V$ is linearly equivalent to zero if the following conditions are satisfied*:

(1) *All the coefficients in Λv are integral.*

(2) *v has degree 0.*

(3) *v is integral and the coefficient of P_d divides $\phi(d, N/d)$.*

(4) *For each i, the number $(e_1 \otimes \cdots \otimes f_i \otimes \cdots \otimes e_k)\Lambda v$ is even, where $e_i = (1, 1, 1, \ldots, 1) \in W_{p_i}^{\vee}$ and $f_i = (0, 1, 0, 1, \ldots) \in W_{p_i}^{\vee}$.*

We use Proposition 1.4 to calculate the order of the elements in C_N. Specifically, for an integral element $v \in V$ of degree zero, the order of v in C_N is the smallest positive integer n such that nv satisfies all the conditions in Proposition 1.4. Notice that if $N = 2^{s_2}M$ where M is a square-free odd integer and $s_2 < 4$ (the case we deal with in this paper), then condition (3) is reduced to the coefficients of v being integral. Therefore, the denominator of $\Lambda(v)$ gives the order of v or half of it.

We can use Proposition 1.4 to calculate the order of elements of C_N considered in Table 1. For example, consider an element $v = v_{p_1} \otimes \cdots \otimes v_{p_k}$, where $v_{p_i} = P_1 + b_i P_{p_i}$, representing an element in C_N when N is square-free and not a prime. This is a generalization of [Ogg 1974] in the case where $N = pq$. Note that

$$\Lambda v = \frac{24}{\prod_i(p_i^2-1)(p_i-1)}(\Lambda_{p_1}v_{p_1} \otimes \cdots \otimes \Lambda_{p_k}v_{p_k})$$

$$= \frac{24}{\prod_i(p_i^2-1)}\left(\begin{pmatrix} p_1-b_1 \\ (p_1-b_1)b_1 \end{pmatrix} \otimes \cdots \otimes \begin{pmatrix} p_k-b_k \\ (p_k-b_k)b_k \end{pmatrix}\right)$$

$$= \frac{24}{\prod_i(p_i+b_i)}\left(\begin{pmatrix} 1 \\ b_1 \end{pmatrix} \otimes \cdots \otimes \begin{pmatrix} 1 \\ b_k \end{pmatrix}\right).$$

Considering the coefficient of the first coordinate, the order is divisible by n, the numerator of the (reduced) fraction $\prod_i(p_i + b_i)/24$. On the other hand, $\Lambda(nv)$

N	Cuspidal element	Order
p	$P_1 - P_p$	$\mathrm{Num}\left(\dfrac{p-1}{12}\right)$
$\displaystyle\prod_{i=1}^{t} p_i$	$(P_1 + b_1 P_{p_1}) \otimes \cdots \otimes (P_1 + b_k P_{p_k})$	$\mathrm{Num}\left(\dfrac{\prod_i (p_i + b_i)}{24}\right)$
	Conditions: $t > 1$; $b_i = \pm 1$ for $i = 1, 2, \ldots, t$; $b_j = -1$ for at least one j.	
$4p$	$P_2 - P_{2p}$	$\dfrac{p-1}{2}$
	Conditions: p is odd.	
$\displaystyle 4\prod_{i=1}^{t} p_i$	$P_2 \otimes (P_1 + b_1 P_{p_1}) \otimes \cdots \otimes (P_1 + b_k P_{p_k})$	$\left(\dfrac{\prod_i (p_i + b_i)}{4}\right)$
	Conditions: $t > 1$; all the p_i are odd; $b_i = \pm 1$ for $i = 1, \ldots, t$; $b_j = -1$ for some j.	
$\displaystyle 8\prod_{i=1}^{t} p_i$	$(P_1 - P_8) \otimes (P_1 + b_1 P_{p_1}) \otimes \cdots \otimes (P_1 + b_k P_{p_k})$	$\dfrac{\prod_i p_i + b_i}{2}$
	Conditions: all the p_i are odd.	

Table 1. Order of elements in C_N. "Num" is the numerator of a reduced fraction.

equals $\binom{1}{b_1} \otimes \cdots \otimes \binom{1}{b_k}$. Therefore

$$(e_1 \otimes \cdots \otimes f_i \otimes \cdots \otimes e_t)\Lambda(nv)$$

is even, implying that nv is linearly equivalent to zero. Hence v has order n. The other entries in Table 1 are calculated the same way.

1C. *Hecke action.* In this section we recall the explicit action of the Hecke operators T_l on the rational cuspidal divisors of $X_0(N)$. This is fairly standard, although the representation of these actions as the tensor product of matrices is not that common. The following is the main result of this section.

Proposition 1.5. (1) *Let $p \nmid N$. Then $T_p : V \to V$ acts as multiplication by $p+1$.*

(2) *Let $p \mid N$ and $V = \bigotimes V_{p_i}$. Then T_p acts trivially on V_{p_i} for $p_i \neq p$, and as*

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ p-1 & 0 & \cdots & 0 & 0 \\ 0 & p & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & p & p \end{pmatrix}$$

on V_p with the standard basis, (the diagonal elements are all 0 except for the first and last, and the subdiagonal elements are all p except for the first).

(3) *For $p|N$ we have w_p acting trivially on V_{p_i} for $p_i \neq p$, and as*

$$\begin{pmatrix} 0 & 0 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 1 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \end{pmatrix} : V_p \to V_p.$$

We will omit the proof of this proposition.

Remark 1.6. Applying w_2 to P_2 when $N = 4M$ with M odd, we see that w_2 has a fixed point on $X_0(4M)$.

We can use this explicit formula to calculate the action of T_p on various elements in the cuspidal subgroup.

Proposition 1.7. *Let $M = \prod p_i$ be an odd square-free integer and $N = 2^a M$ for some $a < 4$. Let $p|N$ and assume that an element $v \in V$ can be written as $v_p \otimes v'$, where $V \simeq V_p \otimes V'$ in an obvious way, $v_p \in V_p$, and $v' \in V'$. Then*

(1) *If $p\|N$ and $v_p = P_1 - P_p$ then $T_p v = v$.*

(2) *If $p\|N$ and $v_p = P_1 + P_p$ then $T_p v = v + u$ where $u = 2(p-1)P_p \otimes v'$.*

(3) *If $p = 2$, $N = 4M$, and $v_2 = P_2$ then $T_2 v = u$ with $u = 2P_4 \otimes v'$.*

(4) *If $p = 2$, $N = 8M$, and $v_2 = P_1 - P_8$ then $T_2 v = u$ where $u = (P_1 + P_2 - 2P_4) \otimes v'$.*

Furthermore if v represents an element in the cuspidal group of order 2, then u is linearly equivalent to 0.

Proof. Calculating the action of various Hecke operators on these elements is a straightforward matrix multiplication. As for proving that u is linearly equivalent to 0, one can check directly that Λu satisfies conditions (1) and (4) of Proposition 1.3, as long as $\Lambda(2v)$ does. □

Corollary 1.8. *Let $v \in V$ be a cuspidal element considered in Table 1. Assume that the order of v in C_N is even and let λ be such that $\lambda v \in C_N[2]$. Then for $p\|N$ (resp. $p = 2$ and $4|N$) we have $T_p(\lambda v) = \lambda v$ (resp. $T_2(\lambda v) = 0$).*

Proof. This follows immediately from Proposition 1.7. □

Remark 1.9. We can also write the elements in Table 1 using the Atkin–Lehner involution. For example, the element $(P_1 - b_1 P_{p_1}) \otimes \cdots \otimes (P_1 - b_1 P_{p_k})$ can be written as $(1 - b_1 w_{p_1}) \cdots (1 - b_k w_{p_k}) P_1$.

Recall that if A is a simple new modular form, then for $p\|N$, $T_p|_A$ is acting as either 1 or -1, and when $p^2|N$ then $T_p|_A = 0$. Hence the corollary tells us that if one of the elements in Table 1 has an even order, then we have a nontrivial element in $C_N[2]$ that is new. This will be used to create congruences between modular forms in later sections.

2. Modular abelian varieties with odd congruence number

In this section we will study simple modular abelian varieties with odd congruence number. By examining the twists of modular abelian varieties, the action of the Atkin–Lehner involutions, and the order of the cuspidal subgroup, we demonstrate that if we have an absolutely simple modular abelian variety with odd congruence number, then its conductor N has at most two prime divisors. We also show that the odd part of N is either square-free or a power of a prime, and if $16|N$, then N is a power of 2. Furthermore, we find some congruences that prime divisors of N must satisfy.

Throughout this section we let A be an optimal modular abelian variety with conductor N and we fix a surjective map $\phi : J_0(N) \to A$ defined over $\mathbb{Z}[1/N]$. Furthermore, let $\pi : X_0(N) \to A$ be the composition of the Albanese embedding and ϕ. As usual, let $\mathbb{T}$ be the Hecke algebra acting on $J_0(N)$ and $S(N)$.

2A. *Atkin–Lehner involution.* The goal of this section is to prove the following:

Theorem 2.1. *Let A be a new simple modular abelian variety with odd modular exponent. If $A(\mathbb{Q})$ has no 2-torsion points, the conductor of A is a power of a prime. Furthermore if A has good reduction at 2 and $A(\mathbb{F}_2)$ has no 2-torsion points, the conductor of A is a power of a prime.*

This theorem was proved by Calegari and Emerton [2009, Theorem 2.1] in the case where A is an elliptic curve. Here, we apply their techniques to higher-dimensional modular abelian varieties.

Lemma 2.2. *Let k be a field and $f : X/k \to Y/k$ be a degree m map between curves. Then the composition*

$$\mathrm{Jac}(Y) \simeq \mathrm{Jac}(Y)^{\vee} \xrightarrow{f^*} \mathrm{Jac}(X)^{\vee} \simeq \mathrm{Jac}(X) \xrightarrow{f_*} \mathrm{Jac}(Y)$$

is multiplication by m.

Proof. It suffices to verify the lemma for the points $(z_1) - (z_2) \in \mathrm{Jac}(Y)$, since these points generate $\mathrm{Jac}(Y)$. Unraveling the definitions we get

$$f_*\big(f^*((z_1) - (z_2))\big) = f_*\bigg(\sum_{f(y_1)=z_1} (y_1) - \sum_{f(y_2)=z_2} (y_2) \bigg)$$

$$= \bigg(\sum_{y_1 \in f^{-1}(z_1)} (z_1) - \sum_{y_2 = f^{-1}(z_2)} (z_2) \bigg) = m((z_1) - (z_2)),$$

where the summations are understood to account for multiplicities.   □

Lemma 2.3. *Let w be an involution on $X_0(N)$. Assume that*

$$
\begin{array}{c}
X_0(N) \\
w \downarrow \qquad \xrightarrow{\ \pi\ } \\
X_0(N)
\end{array}
\xrightarrow{\ \pi\ } A
$$

commutes. Then the modular exponent of A is even.

Proof. The assumptions imply that π factors through

$$ X_0(N) \longrightarrow X_0(N)/w \longrightarrow A. $$

Therefore ϕ factors through

$$ \mathrm{Jac}(X_0(N)) \longrightarrow \mathrm{Jac}(X_0(N)/w) \longrightarrow A. $$

Dualizing this diagram and using the autoduality of $J_0(N)$, we get

$$
\begin{array}{ccccc}
A^\vee & \longrightarrow & \mathrm{Jac}(X_0(N)/w)^\vee & \longrightarrow & J_0(N)^\vee \\
\delta \downarrow & & \downarrow & & \downarrow \\
A & \longleftarrow & \mathrm{Jac}(X_0(N)/w) & \longleftarrow & J_0(N).
\end{array}
$$

By [Lemma 2.2](), the middle arrow is multiplication by 2, since the degree of $X_0(N)$ $\to X_0(N)/w$ is 2. Using the commutativity of this diagram, we can see that $A^\vee[2] \subset \ker(\delta)$. Recalling that the modular exponent is the exponent of the kernel of δ, we conclude that the modular exponent of A is even. $\square$

Recall that for an involution map $w : X_0(N) \to X_0(N)$, we get the induced map $w_* : J_0(N) \to J_0(N)$. Let A be an optimal modular abelian variety, and $\phi : J_0(N) \to A$ the associated surjective map. Then if w_* keeps $\ker(\phi)$ invariant, then w_* acts on A as well (this happens when, for example, w is an Atkin–Lehner involution and A is new). The following lemma deals with the case when w_* is trivial on A.

Lemma 2.4. *Let k be either $\mathbb{Q}$ or $\mathbb{F}_p$ with $p \nmid N$. Let A be an optimal modular abelian variety with odd modular exponent. As before let $\pi : X_0(N) \to A$ be the composition of Albanese embedding $X_0(N) \to J_0(N)$ and ϕ. Assume that for some involution w, $w_* : J_0(N) \to J_0(N)$ descends down to a trivial action on A. Then $\pi(w(z)) - \pi(z)$ is a nontrivial k-rational 2-torsion point for all $z \in X_0(N)(\bar{k})$.*

Proof. Recall that P_1 is the cusp at infinity and $\pi(z) = \phi(z - P_1)$. Then we get

$$
\begin{aligned}
\pi(w(z)) - \pi(z) &= \phi(w(z) - P_1) - \phi(z - P_1) \\
&= \phi(w(z) - w(P_1)) - \phi(z - P_1) + \phi(w(P_1) - P_1) \\
&= w_*(\phi(z - P_1)) - \phi(z - P_1) + \phi(w(P_1) - P_1) = \pi(w(P_1)).
\end{aligned}
$$

Therefore $\pi(w(z)) = \pi(z) + \pi(w(P_1))$ for all $z \in X_0(N)$. Applying this equa-
tion to $w(z)$ we get $\pi(w(w(z))) = \pi(w(z)) + \pi(w(P_1)) = \pi(z) + 2\pi(w(P_1))$.
Therefore, $2\pi(w(P_1)) = 0$. By Lemma 2.3, if A has odd modular exponent, then
$\pi(w(z)) - \pi(z)$ is nontrivial. Thus, $\pi(w(P_1))$ is a nontrivial 2-torsion point of A.
It is k-rational because $w(P_1)$ is also k-rational.   □

Proof of Theorem 2.1. Let W be the group of Atkin–Lehner involutions on $X_0(N)$,
and let $k = \mathbb{Q}$ or $\mathbb{F}_2$ when N is odd. Since we are assuming that A is new and
simple, for any Atkin–Lehner involution $w \in W$, we have $w_*(z)$ is either z or $-z$
for all $z \in A(\bar{k})$. This gives us a group homomorphism $W \to \{\pm 1\}$. Let W_0 be
the kernel of this map. Note that W_0 has index at most 2 in W. Assume that N is
not a power of a prime; hence W will have more than 2 elements. Therefore, we
can find a nontrivial element $w \in W_0$; then $w_*(z) = z$ for all $z \in A(\bar{k})$. Applying
Lemma 2.4, we find that $0 \neq \pi(w(P_1)) \in A[2](k)$. Therefore, if $A[2](k) = 0$ then
N must be a power of a prime.   □

Lemma 2.4 can also be used to find the signs of the Atkin–Lehner involutions
on A in certain cases.

Lemma 2.5. *Let A be a new modular simple abelian variety with conductor N
and odd modular exponent. If the Atkin–Lehner involution $w_r : X_0(N) \to X_0(N)$
has a fixed point then $(w_r)_*$ acts as -1 on A. Specifically, $(w_N)_*$ acts as -1 on A.
When $N = 2M$ (resp. $N = 4M$), $(w_2)_*$ acts as 1 (resp. $(w_2)_*$ acts as -1) on A.*

Proof. Let $P \in X_0(N)(\bar{\mathbb{Q}})$ be the fixed point of w_r. Then $\pi(P) = \pi(w_r(P))$,
which implies that $\pi(w_r(P)) - \pi(P) = 0$. However, we know that if $(w_r)_* = 1$
then $\pi(w_r(z)) - \pi(z) = \pi(w_r(P_1))$ for any $z \in X_0(N)(\bar{\mathbb{Q}})$. Specifically, we get
$\pi(w_r(z)) = \pi(z)$, which by Lemma 2.3 implies that A has an even congruence
number. Therefore $(w_r)_* = -1$ when w_r has a fixed point in $X_0(N)$.

Finally, the point $\sqrt{-N}$ is fixed by w_N. When $N = 2M$, we can check that
$1/(M - i\sqrt{M})$ is fixed under $(w_M)_*$. Similarly, when $N = 4M$, P_2 is fixed under
$(w_2)_*$. Therefore, we have the desired result.   □

Since $(w_N)_*$ is the sign of the functional equation, we get the following:

Corollary 2.6. *If A is a simple modular abelian variety with odd congruence num-
ber, then the analytic rank of A is even.*

Remark 2.7. Calegari and Emerton used Theorem 2.1 for modular elliptic curves
E with odd modular degree and conductor N to show that N has at most two odd
prime divisors. Specifically, since $E[2](\mathbb{Q})$ has at most 4 elements, an immediate
corollary of Theorem 2.1 is that if N has more than 3 prime divisors, then E has
even modular degree. Similarly, if E has good reduction at 2, then since $E[2](\mathbb{F}_2)$
has at most two elements, they conclude that if N has more than two prime divisors
then E has even modular degree.

2B. *Nonsemistable case.* The goal of this section is to prove the following:

Theorem 2.8. *Let A be an absolutely simple modular abelian variety A of level N with odd congruence number. Let $\delta_p = 0$ for the odd primes p and $\delta_2 = 2$. Assume that $p^{2+\delta_p}|N$. Then A has good reduction away from p and 2, and has potentially good reduction everywhere. Specifically, if p is odd and $p^2|N$, then $N = p^s$, $N = 4p^s$, or $N = 8p^s$ for $s \geq 2$, and if $16|N$ then $N = 2^s$.*

We expect this theorem to be true without assuming A to be absolutely simple; however, at this moment we do not know how to overcome the difficulty with the inner forms in that case. To prove this theorem, we use the technique of [Calegari and Emerton 2009] to show that such modular abelian varieties have inner twists or complex multiplication by a character of conductor p. Using the results of [Ribet 1981] on inner twists, we will prove that A must have potentially good reduction everywhere if A is absolutely simple, and that A has good reduction away from p, and possibly 2. We have the following lemma.

Lemma 2.9. *If $\operatorname{End}_{\overline{\mathbb{Q}}}(A) \otimes \mathbb{Q}$ is a matrix algebra, then A is not absolutely simple.*

Proof. Assume that $R = \operatorname{End}_{\overline{\mathbb{Q}}}(A) \otimes \mathbb{Q}$ is a matrix algebra. We can find the projections $e_1, e_2 \in R$ such that $e_1 + e_2 = \operatorname{Id}$, $e_1 e_2 = 0$, and $e_1, e_2 \notin \{0, \operatorname{Id}\}$. For some integer n, $n e_i \in \operatorname{End}_{\overline{\mathbb{Q}}}(A)$. If we assume that A is absolutely simple, the image of $n e_i A$ must be A or 0. However, since the product of $n e_1$ and $n e_2$ equals $n^2 e_1 e_2 = 0$, one of them must be 0. Assume without loss of generality that $n e_2 = 0$ in $\operatorname{End}_{\overline{\mathbb{Q}}}(A)$. This implies that $e_2 = 0$, which contradicts the assumption $e_2 \notin \{0, \operatorname{Id}\}$. Therefore, A is not absolutely simple. $\square$

This lemma is used in conjunction with Ribet's result on the endomorphism algebra of modular abelian varieties with inner twists. Specifically, let A be a d-dimensional simple modular abelian variety. There are d modular eigenforms of weight 2 and level N associated with A, which are Galois conjugate to each other. Let $f = \sum a_n q^n$ be one such eigenform and let $E = \mathbb{Q}(\ldots, a_n, \ldots)$ be the field of definition of f. We know that $\operatorname{End}_{\mathbb{Q}}(A) \otimes \mathbb{Q} = E$. Let

$$D = \operatorname{End}_{\overline{\mathbb{Q}}}(A) \otimes \mathbb{Q}$$

be the algebra of endomorphisms of A. From [Ribet 1980] we know that E is its own commutant in D, and therefore D is a central simple algebra over some subfield F of E. If we assume that A is absolutely simple, then D must be some division algebra with centre E. Furthermore, D must be either E (which forces $E = F$) or a quaternion division algebra over F (which forces E to be a quadratic extension of F).

Proposition 2.10. *Let A be an absolutely simple modular abelian variety A of level N with odd congruence number. Let $\delta_p = 0$ for odd primes and $\delta_2 = 2$. If*

$p^{2+\delta_p}|N$, *then A has a complex multiplication or an inner twist and A has potentially good reduction everywhere. Specifically, for any other prime number q if* $q|N$ *then* $q^2|N$.

Proof. Assume that A is of dimension d, and let

$$f_A = \sum a_n q^n \in \mathbb{C}((q))$$

be a normalized eigenform associated with A. Let $E = \mathbb{Q}(\ldots, a_i, \ldots) \subset \mathbb{C}$. Let χ be the quadratic character with conductor p. Since $p^{2+\delta_p}|N$, $\chi \otimes f_A$ is another modular eigenform in $S_2(\Gamma_0(N))$ (see [Shimura 1971]). Since χ is a quadratic character, χ takes values in ± 1, and as a result $\chi \otimes f_A \equiv f_A \pmod{\lambda}$ for any $\lambda|2$. If A has odd congruence number, then $\chi \otimes f_A$ must be in the same conjugacy class as f_A. If $\chi \otimes f_A = f_A$, then A has complex multiplication by χ, and therefore A has potentially good reduction everywhere. In this case, A must be an elliptic curve, because if A has complex multiplication and has a dimension greater than 1, then the ring of endomorphisms of A is a matrix algebra, which contradicts the absolute simplicity assumption. In general, A might have an inner twist, and $\chi \otimes f_A = \gamma(f_A)$ for some $\gamma \in \mathrm{Hom}(E, \mathbb{C})$. Let $\Gamma \subset \mathrm{Hom}(E, \mathbb{C})$ such that for any $\gamma \in \Gamma$ we can find a character χ_γ such that $\chi_\gamma \otimes f_A = \gamma(f_A)$. By [Ribet 1981], $F = E^\Gamma$ and (as discussed above) $D = \mathrm{End}_{\bar{\mathbb{Q}}} A \otimes \mathbb{Q}$ must be a quaternion algebra. However, using [Ribet 1980, Theorem 3], A has potentially good reduction everywhere, as desired.

The final claim of the lemma follows by noting that if $q|N$ but $q^2 \nmid N$, then A has multiplicative reduction over any field extension. $\qquad\square$

Proof of Theorem 2.8. Assume that $p^{2+\delta_p}|N$ and $q^{2+\delta_q}|N$ for distinct primes p and q. In this case, assuming that A has no complex multiplication, A has more inner twists, and the subset $\Gamma \subset \mathrm{Hom}(E, \mathbb{C})$ will have at least four elements, γ_1, γ_p, γ_q, and γ_{pq}. But that means that $|E : F| \geq 4$, which shows that D must be a matrix algebra. However, Lemma 2.9 forces A not to be absolutely simple, which contradicts our assumption. Since we are assuming A is absolutely simple if A has complex multiplication, then A is an elliptic curve. Therefore it will have complex multiplication by χ_p and χ_q, which is impossible. $\qquad\square$

2C. *Number of primes of bad reduction.* We now show that a modular abelian variety with odd congruence number has bad reduction at no more than two primes. Let A be an absolutely simple optimal abelian variety of conductor N. Let $B = \ker(\phi)$ where ϕ is the modular uniformization map $\phi : J_0(N) \to A$. Assume that N is a not a power of a prime. Then Theorem 2.1 says that $A[2](\mathbb{Q})$ has a nontrivial element. Let $z \in A[2](\mathbb{Q})$ be a nontrivial rational 2-torsion point of A, and let $\mathfrak{m} \subset \mathbb{T}$ be the annihilator of z. Since $z \in A[\mathfrak{m}] \neq 0$, we get that $A^\vee[\mathfrak{m}] \neq 0$. Therefore, if $B[\mathfrak{m}] \neq 0$ as well, then A will have an even congruence number. We will show that when N has more than two prime divisors, then $B[\mathfrak{m}] \neq 0$.

Lemma 2.11. *Let A be a new simple modular abelian variety, $0 \neq z = A[2](\mathbb{Q})$, and let $\mathfrak{m}$ be the annihilator of z in $\mathbb{T}$. Then $\mathfrak{m}$ is generated by 2, $T_l - (l+1)$ for $l \nmid N$, $T_p - 1$ for $p|N$ but $p^2 \nmid N$, and T_p for $p^2|N$.*

Proof. Clearly z is killed by 2, and since A is a new modular abelian variety, if $p\|N$, we have $T_p(z) = \pm z = z$, and if $p^2|N$ then $T_p(z) = 0$. Let ρ be the Galois representation

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{T}/\mathfrak{m}).$$

Since A has a rational 2 torsion point,

$$\rho \simeq \begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix},$$

where χ is the cyclotomic character. Therefore $\mathrm{trace}(\rho(\mathrm{Frob}(l))) = 1 + \chi(l) = l+1$ for $l \nmid 2N$, and hence by the Eichler–Shimura relationship we get that $T_l - (l+1) \in \mathfrak{m}$ for $l \nmid 2N$. When $l = 2$ and N is odd, by Theorem 2.1 we get that A has ordinary reduction at 2, and hence $T_2 \notin \mathfrak{m}$, or equivalently $T_2 - (2+1) \in \mathfrak{m}$. □

Recall that $C_N \subset J_0(N)$ is the rational cuspidal subgroup of $J_0(N)$. Let $\mathfrak{m} \subset \mathbb{T}$ be the annihilator of $z \in A[2]$. We can use the elements considered in Table 1 to show that $B[\mathfrak{m}] \neq 0$ when N has more than two prime divisors. Specifically, if $v \in C_N$ of even order is such that $\phi(v) = 0$, then $v \in B \cap C_N$. If v is also a cusp of the type considered in Table 1 and of even order, then by Corollary 1.8 we get that for some integer λ we have that $\lambda v \in C_N[\mathfrak{m}]$. Therefore, to show that A has an even congruence number, we only need to check that such v's have even order and that $\phi(v) = 0$.

Theorem 2.12. *Let A be a new absolutely simple optimal modular abelian variety with odd congruence number. Then N has at most two prime factors.*

Proof. If A has an inner twist or complex multiplication, then the result follows by Theorem 2.8. Assume that A has odd congruence number with no inner twist or complex multiplication. Assume to the contrary that N has more than two prime factors. Then $N = 2^\alpha M$ with M a square-free odd integer, and $\alpha < 4$. Furthermore, by Theorem 2.1, we can find a nontrivial $z \in A[2](\mathbb{Q})$. Let $\mathfrak{m}$ be the annihilator of z. We will consider three main cases, based on the valuation of N at 2.

Assume that $4 \nmid N$. Since $w_N = \prod_{l|N} w_l$, and $(w_N)_* = -1$, there is an odd number of primes such that $(w_l)_*$ act as -1 on A. Therefore, we can select three distinct prime divisors of N — call them p, q, and r — such that $(w_p)_*$ acts as -1, while $(w_r)_* = (w_q)_*$. If $2\|N$, by Lemma 2.5 $(w_2)_*$ acts as $+1$. Therefore, without loss of generality assume that $2 \nmid pq$.

Let $s_p, s_q = \pm 1$ and let

$$v = (1 - w_{qr})(1 + s_p w_p)(1 + s_q w_q)P_1 = (1 + s_p w_p)(1 + s_q w_q)(1 - s_q w_r)P_1.$$

Consulting Table 1 we get that v has order $\mathrm{Num}\big((1+s_p p)(1+s_q q)(1-s_q r)/24\big)$. If we select $s_p \equiv -p \pmod 4$ and $s_q \equiv -q \pmod 4$, then this order is even. Next we show that $\phi(v) = 0$. Note that $\pi(w_{qr}(\tau)) = \pi(\tau) + a$ for any $\tau \in X_0(N)$, where a is some 2-torsion point. Let $P = (1 + s_p w_p)(1 + s_q w_q) P_1 = P_1 \pm P_p \pm P_q \pm P_{pq}$. Then

$$\phi(v) = \phi(w_{qr}(P) - P) = \sum_{m \mid pq} \pi(w_{qr}(P_m)) - \pi(P_m) = 4a = 0,$$

which shows that A has an even congruence number.

Assume that $4 \| N$. By Lemma 2.5 we know that $(w_2)_*$ acts as -1. Let $p, q \mid N$ and let $v = (1 - w_p)(1 + s_q w_q) P_2$ with $s_q = \pm 1$. From Table 1 we get that the order of v is $\mathrm{Num}\big((1 - p)(1 + s_q q)/4\big)$. If we select $s_q \equiv -q \pmod 4$, then v will have an even order. Since $(w_2)_*$ is acting as -1, either $(w_p)_*$ or $(w_{2p})_*$ is acting trivially on A. Let w be the corresponding Atkin–Lehner involution. Note that because $w_2(P_2) = P_2$, $v = (1 - w)(1 + s_q w_q) P_2$. Furthermore, $\pi(w(\tau)) - \pi(\tau) = a \in A[2]$ for any $\tau \in X_0(N)$. As a result,

$$\phi(v) = \pi(P_2) - \pi(w(P_2)) + s_q(\pi(P_{2q}) - \pi(w(P_{2q}))) = a + s_q a = 0.$$

Therefore $\phi(v) = 0$, which proves that in this case A has an even congruence number.

Finally assume that $8 \| N$, and let $p, q \mid N$ be two distinct odd divisors of N. Let $(w_p)_*$ and $(w_q)_*$ act as s_p and s_q on A. Let

$$v = (1 - w_2)(1 + s_p w_p)(1 + s_q w_q) P_1 = (1 - w_2)(1 + s_p s_q w_{pq})(1 + s_p w_p) P_1.$$

Then, again from Table 1, v has order $\mathrm{Num}\big((1 + s_p p)(1 + s_q q)/2\big)$ that is even. Note that, similar to the case when N is odd, we can write $v = (1 - w)P$ for some Atkin–Lehner involution w such that $w_* = 1$ and some $P = (1 - w_2)(1 \pm w')P_1$. That shows $\phi(v) = 0$. Therefore A in this case will have an even congruence number again. □

Combining this result with Theorem 2.8, we get:

Corollary 2.13. *Let A be an absolutely simple modular abelian variety with odd congruence number and conductor N. Then N has at most two prime divisors. Furthermore, if N is not square-free, then $N = 2^a$, p^b, $4p^b$, or $8p^b$, where p is an odd prime.*

2D. *Congruence classes of primes.* Let A be a simple modular abelian variety of conductor N with odd congruence number, and without complex multiplication or an inner twist. As usual let $\pi : X_0(N) \to A$ to be the composition of the Albanese embedding with the modular uniformization ϕ. Assume that N is not a power of a prime, which by Theorem 2.1 implies that $A[2](\mathbb{Q})$ is nontrivial. From the previous

sections we know that N has at most two prime factors, say p and q. In this section we find congruences that p and q must satisfy. As in the proof of Theorem 2.12, we use different techniques depending on the valuation of N at 2.

If N is odd, then $N = pq$ with both p and q being odd. By Lemma 2.5, we know that $(w_{pq})_*$ is acting as -1 on A. Therefore, assume without loss of generality that $(w_q)_*$ is acting trivially on A and $(w_p)_*$ is acting as -1. Let $v = (1 \pm w_p)(1 - w_q)P_1$. Again, $\pi(\tau) - \pi(w_q(\tau)) = a \in A[2]$ for all $\tau \in X_0(N)$. As a result,

$$\phi(v) = \pi(P_1) - \pi(w_q(P_1)) \pm (\pi(P_p) - \pi(w_q(P_p))) = a \pm a = 0.$$

Note that the order of v is $\mathrm{Num}((p \pm 1)(q - 1)/24)$. Since we are assuming that A has odd congruence number, we get that $p \equiv \pm 3 \pmod 8$ and $q \equiv 3 \pmod 4$.

Corollary 2.14. *Let A be a modular abelian variety with odd congruence number and conductor pq, where p and q are odd. Then $A[2](\mathbb{Q})$ is at least 2-dimensional over $\mathbb{F}_2$.*

Proof. We prove this by finding two distinct points in $C_N[\mathfrak{m}]$. First note that $P_1 - P_p$ has order $(p - 1)(q^2 - 1)/24$ and $P_1 - P_q$ has order $(p^2 - 1)(q - 1)/24$. Therefore, both

$$u = \frac{(p - 1)(q^2 - 1)}{48}(P_1 - P_p) \quad \text{and} \quad u' = \frac{(p^2 - 1)(q - 1)}{48}(P_1 - P_q)$$

are of order 2. We can easily check that $T_p u = u$ and $T_q u' = u'$. On the other hand,

$$u + T_q u = \frac{(p - 1)(q^2 - 1)}{48}(P_1 - P_p + P_q - P_{pq}),$$

which is zero. Similarly, we get $u' + T_p u' = 0$. Therefore, $u, u' \in C_N[\mathfrak{m}]$. Furthermore, we know that $\Lambda(u + u')$ has integral coefficients, but

$$(1, 0) \otimes (1, 1)\Lambda(u + u') = (q - 1)/2,$$

which is not even since $q \equiv 3 \pmod 4$. Therefore, $u + u' \neq 0$, which implies that $C_N[\mathfrak{m}]$ is at least 2-dimensional over $\mathbb{F}_2$. Since we are assuming that A has odd congruence number, $C_N[\mathfrak{m}]$ injects in A, which is the desired result. $\square$

If $N = 2p$, we know by Lemma 2.5 that $(w_2)_*$ acts trivially and $(w_p)_*$ acts as -1 on A. Therefore, $\pi(P_2) = \pi(w_2(P_1)) \in A[2]$, and $P_2 - P_1$ (which has order $(p^2 - 1)/8$) must have an even order. Let $v = ((p^2 - 1)/16)(P_2 - P_1) \in C_N[2]$. By Corollary 1.8 we get $v \in C_N[\mathfrak{m}]$. Note that

$$\phi(v) = \pi\left(\frac{p^2 - 1}{16}(P_2 - P_1)\right) = \frac{p^2 - 1}{16}\pi(P_2),$$

so if $(p^2 - 1)/16$ is even, then $\pi(v) = 0$. This implies that $v \in C_N[\mathfrak{m}] \cap B$, and, in turn, that the congruence number is even. Since we are assuming that

the congruence number of A is odd, we get that $(p^2 - 1)/16$ is odd; that is, $p^2 - 1 \equiv 16 \pmod{32}$. That implies that $p \equiv \pm 7 \pmod{16}$. However, we also know that w_2 cannot have any fixed points. This implies that -2 is not a quadratic residue mod p, which means that $p \equiv 5, 7, 13,$ or $15 \pmod{16}$. Therefore $p \equiv 7 \pmod{16}$.

If $N = 4p$, then we know that $(w_2)_*$ acts as -1 on A, while $(w_p)_*$ acts trivially. Therefore, $\pi(P_2) - \pi(P_{2p}) = \pi(P_2) - \pi(w_p(P_2)) \in A[2]$. The order of $P_2 - P_{2p}$ is $(p-1)/2$. Therefore, if A has odd congruence number, $(p-1)/4$ must be odd, hence $p \equiv 5 \pmod 8$.

If $N = 8p$, we can check that $(1 - w_2)(1 - w_p)P_1$ vanishes in A, and that it has order $(p-1)/2$. Therefore, $4 \nmid p - 1$, otherwise A will have an even congruence number. Therefore $p \equiv 3 \pmod 4$. (We can probably say more, if we figure out the sign of $(w_p)_*$.)

We combine the above results in the following theorem.

Theorem 2.15. *Let A be a new modular abelian variety with odd congruence number and conductor N. Assume that A has no inner twists or complex multiplications. Then one of the following must be true.*

(1) *N is a prime number p.*

(2) *$N = pq$ and $p \equiv \pm 3 \pmod 8$ and $q \equiv 3 \pmod 4$.*

(3) *$N = 2p$ and $p \equiv 7 \pmod{16}$.*

(4) *$N = 4p$ and $p \equiv 5 \pmod 8$.*

(5) *$N = 8p$ and $p \equiv 3 \pmod 4$.*

3. Elliptic curves with odd congruence number

In this section, we apply the results of the previous section to the case of elliptic curves. We show that the conductors of all such elliptic curves are of the form p, pq, $2p$, $4p$, or one of the finitely many exceptions. We study each class to demonstrate that all such elliptic curves have finite Mordell–Weil group, except possibly when the conductor is prime. Furthermore, we know from the result of [Agashe et al. 2008] that when $4 \nmid N$, then having odd congruence number is the same as having odd modular degree. As a result, we can state many of our results in terms of modular degrees. We conjecture that in fact having odd congruence number is equivalent to having odd modular degree in all cases.

Complex multiplication. Let E be an elliptic curve of conductor N. If $p^2 | N$ for an odd prime p, then by Section 2B we know that E has complex multiplication. We also showed that if $16 | N$ then E must have complex multiplication. There are only finitely many elliptic curves over rationals with complex multiplication and the conductor $2^m p^n$ for some prime number p. The following is the list of all such

elliptic curves that have odd modular degree: $E = 27A, 32A, 36A, 49A, 243B$. We also verify that all such elliptic curves have rank 0, as predicted by Watkins' conjecture.

We will now focus our attention on elliptic curves without complex multiplication, that is, elliptic curves with conductor $N = p, 2p, 4p, 8p$, or pq for some odd primes p and q. Each of the remaining sections deals with one of these remaining cases.

Prime level. Let E be an elliptic curve with odd congruence number and a prime conductor N. Mestre and Oesterlé [1989] have studied the elliptic curves of prime conductors, and they have demonstrated that aside from elliptic curves $11A$, $17A$, $19A$, and $37B$, all such elliptic curves have either a trivial torsion subgroup or a $\mathbb{Z}/2\mathbb{Z}$ torsion subgroup. The above cases have the torsion structures $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, and $\mathbb{Z}/3\mathbb{Z}$, respectively. Mestre and Oesterlè also showed that if E_{tors} is $\mathbb{Z}/2\mathbb{Z}$, then E is a Neumann–Setzer curve and $N = u^2 + 64$. Stein and Watkins [2004] have studied the parity of congruence numbers of Neumann–Setzer curves and they show that E has odd congruence number if and only if $u \equiv 3 \pmod 8$. Furthermore one can show that Neumann–Setzer curves have rank 0 using descent. We will give another proof of this fact using L-functions.

Proposition 3.1. *Let E be an elliptic curve over $\mathbb{Q}$ with a prime conductor N. Assume that E_{tors} is nontrivial. Then $L(E, 1) \neq 0$, hence $E(\mathbb{Q})$ has rank 0.*

Proof. Recall that

$$L(E, 1) = 2\pi i \int_0^{i\infty} f_E(z)\, dz \equiv \pi(P_N) \pmod{\Lambda_E},$$

where $\mathbb{C}/\Lambda_E \simeq E(\mathbb{C})$. Therefore, if $L(E, 1) = 0$, then $\pi(P_N) = 0$, or alternatively $\phi(P_1 - P_N) = 0$. By [Mazur 1977; Mestre and Oesterlé 1989] (see also [Emerton 2003]) we know that $J_0(N)_{\text{tors}}$ is generated by the cusp $P_1 - P_N$, and for any elliptic curve quotient of $J_0(N) \to E$, E_{tors} is generated by the image of $\pi(P_1) - \pi(P_N)$. Since we are assuming that E has a nontrivial torsion structure, $\pi(P_1) - \pi(P_N) \neq 0$, which implies that $L(E, 1) \neq 0$. Therefore the rank of $E(\mathbb{Q})$ is zero by [Kolyvagin 1988; Gross and Zagier 1986]. □

The case when E has trivial torsion structure and odd congruence number was studied in [2009], where it is shown that E has an even analytic rank (since $(w_N)_* = -1$), supersingular reductions at 2 and $E(\mathbb{R})$ is connected. From a search in Cremona's database, it appears that if an elliptic curve E has supersingular reduction at 2, Mordell–Weil rank 0, and a connected real component, then E will have odd congruence number.

Level $N = pq$. We consider elliptic curves of odd modular degree and conductor $N = pq$, where p and q are both odd primes. Let E be such an elliptic curve. Assume throughout this section that $(w_p)_* = -1$ on E. By Theorem 2.15, we know that $p \equiv \pm 3 \pmod 8$ and $q \equiv 3 \pmod 4$. We will show that with a few exceptions, $p, q \equiv 3 \pmod 8$, and that all such elliptic curves have finite Mordell–Weil group over $\mathbb{Q}$.

Recall that by Corollary 2.14 we know that $E[2](\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z})^2$. First, we show that if E_{tors} is $\mathbb{Z}/2 \times \mathbb{Z}/4$, then E has conductor 15 or 21. We can prove a general result about semistable elliptic curves with $E_{\text{tors}} = \mathbb{Z}/2 \times \mathbb{Z}/4$ and good reduction at 2:

Lemma 3.2. *Let E be a semistable elliptic curve with good reduction at 2. $E_{\text{tors}} = \mathbb{Z}/2 \times \mathbb{Z}/4$, and let $Q \in E(\mathbb{Z}[1/N])$ be a point of order 4. Let $\bar{Q}$ be the reduction of Q mod 2. Then $\bar{Q}$ has order 4 in $E(\mathbb{F}_2)$.*

Proof. We can check that an elliptic curve E with good reduction at 2 and a rational 2-torsion point has a minimal model

$$E : y^2 + xy = x^3 + a_2 x^2 + a_4 x.$$

Since $E[2] = \mathbb{Z}/2 \times \mathbb{Z}/2$, $(4a_2 + 1)^2 - 64a_4$ is a perfect square. The x coordinates of the 2-torsion points are 0, 4α, and $\beta/4$, where α and β are both (odd) integers since we are assuming that E is in minimal model. Since E is assumed to be semistable, α and β are coprime. Note that the point $(\beta/4, -\beta/8) \in E(\mathbb{Q})$ maps to the identity under the reduction mod 2 map. Using the notation of [Silverman 1992], we have

$$b_2 = 16\alpha + \beta, \quad b_4 = 2\alpha\beta, \quad b_6 = 0, \quad b_8 = -\alpha^2\beta^2, \quad \Delta = \alpha^2\beta^2(16\alpha - \beta)^2.$$

Let $Q \in E(\mathbb{Q})$ be a point of order 4, and let $x(Q) = x_0$. Recall that we want to show $\bar{Q} \in E(\mathbb{F}_2)$ is a point of order 4. We have that $x([2]Q) = 0$, 4α, or $\beta/4$. If $\bar{Q}$ has order less than 4, then $2\bar{Q}$ must be the identity element, that implies that $x([2]Q) = \beta/4$. In that case

$$\frac{\beta}{4} = \frac{x_0^4 - b_4 x_0^2 - b_8}{4x_0^3 + b_2 x_0^2 + 2b_4 x_0} = \frac{x_0^4 - 2\alpha\beta x_0^2 + \alpha^2\beta^2}{4x_0^3 + (16\alpha + \beta)x_0^2 + 4\alpha\beta x_0},$$

so

$$0 = x_0^4 - \beta x_0^3 - \left(6\alpha\beta + \frac{\beta^2}{4}\right)x_0^2 - \alpha\beta^2 x_0 + \alpha^2\beta^2 = \left(x_0^2 - \frac{\beta}{2}x_0 + \alpha\beta\right)^2 - \left(4\alpha\beta + \frac{\beta^2}{2}\right)x_0^2.$$

Therefore, $16\alpha\beta + 2\beta^2 = 2\beta(8\alpha + \beta)$ must be a perfect square; however that is not possible because α and β are odd. As a result, $x([2]Q) = 0$ or 4α. Therefore, $[2]\bar{Q}$ has order 2 in $E(\mathbb{F}_2)$. This shows that $\bar{Q}$ has order 4, which is the desired result. $\square$

Proposition 3.3. *Let E be an elliptic curve with conductor pq and torsion group $\mathbb{Z}/2 \times \mathbb{Z}/4$. Then $pq = 15$ or 21.*

Proof. Using the same notation as in Lemma 3.2, let 0, 4α, and $\beta/4$ be the x-coordinates of the 2-torsion points of E. Let Q be a point in E_{tors} of order 4. By Lemma 3.2, $x([2]Q) = 0$ or 4α. Without loss of generality, assume that $x([2]Q) = 0$, since if $x([2]Q) = 4\alpha$, then we can change the coordinates to find another model with $x([2]Q') = 0$. Let $x_0 = x(Q)$. Then $x_0^4 - 2\alpha\beta x_0^2 + \alpha^2\beta^2 = 0$, which implies that $x_0^2 = \alpha\beta$. Since α and β are coprime, they are both perfect squares, or negatives of perfect squares (both of the same sign). Since E is of conductor pq, $\Delta = \alpha^2\beta^2(16\alpha - \beta)^2$ is a product of the powers of p and q. Let $a^2 = \pm\alpha$ and $b^2 = \pm\beta$. Then, $a^4 b^4 (4a - b)(4a + b)$ is a product of the powers of p and q. Note that $(4a - b, 4a + b) = 1$, which implies that all factors are pairwise coprime. Note that if $|4a + b| = |4a - b| = 1$, then either $a = 0$ or $b = 0$ contrary to our assumptions. Therefore we will assume without loss of generality that $4a + b > 1$.

If $4a - b \neq \pm 1$, then $a^2 = b^2 = 1$, which means E is the elliptic curve 15A. If $4a - b = \pm 1$ then $|b| > 1$; therefore $|a| = 1$. Since we are assuming that $4a + b > 1$ we get that $a = 1$, and $4a - b = 1$ leads to elliptic curve 21A and $4a - b = -1$ leads to elliptic curve 15A. This completes our proof.   □

Remark 3.4. Note that the previous proposition seems a bit tedious. It is straightforward to show that 3 must divide the conductor by the Hasse–Weil bound. Unfortunately, it is not clear how this observation can simplify the argument.

An immediate corollary of the above is that for an elliptic curve E of conductor pq and ordinary reduction at 2, we have $E_{\text{tors}} = (\mathbb{Z}/2\mathbb{Z})^2$, since the only other option is $E_{\text{tors}} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. However the Hasse–Weil bounds for elliptic curves rule this case out.

Theorem 3.5. *Assume that E is an elliptic curve with odd modular degree. Furthermore, assume that the conductor of E is pq with $pq \neq 21$ or 15. Then $p, q \equiv 3 \pmod 8$.*

Proof. By Corollary 2.14 we know that $E[2](\mathbb{F}_2)$ is nontrivial, hence E has good ordinary reduction at 2. Therefore, for $pq \neq 21$ and 15 we have $E(\mathbb{Q})_{\text{tors}} = (\mathbb{Z}/2\mathbb{Z})^2$. Recall that we are assuming $(w_p)_* = -1$ and $(w_q)_* = 1$ on E. Note that

$$\pi(\tau) - \pi(w_p(\tau)) = \phi(\tau - P_1) - \phi(w_p(P_1) - P_1) - \phi(w_p(\tau) - w_p(P_1))$$
$$= \pi(\tau) - (w_p)_*(\pi(\tau)) - \pi(w_p(P_1)) = 2\pi(\tau) - \pi(P_p),$$

for any $\tau \in X_0(N)$. When τ is a cusp of $X_0(N)$, $\pi(\tau)$ is a torsion point, and since $E_{\text{tors}} = E[2]$ we get $2\pi(\tau) = 0$. Therefore

$$\pi(\tau) - \pi(w_p(\tau)) = \pi(P_p).$$

Let $v = (1 + w_q)(1 - w_p)P_1$. Then

$$\phi(v) = \big(\pi(P_1) - \pi(w_p(P_1))\big) + \big(\pi(P_q) - \pi(w_q(P_q))\big) = 2\pi(P_p) = 0.$$

As a result, $v \in B \cap C_N$. Therefore, by Corollary 1.8, if v has even order then E will have an even congruence number. Since we are assuming that E has odd congruence number, v must have odd order. The order of this point is $\mathrm{Num}((q+1)(p-1)/24)$. Since $q \equiv 3 \pmod 4$, $4|q+1$. If $p \equiv -3 \pmod 8$, then v will have an even order, and E will have an even congruence number. Therefore $p \equiv 3 \pmod 8$, and $2\|p+1$. If $q \equiv -1 \pmod 8$, again v will have an even order. Therefore, $q \equiv 3 \pmod 8$, which is the desired result. $\qquad\square$

We also get the following corollary.

Corollary 3.6. *Assume that E is an elliptic curve with odd congruence number and conductor pq with $pq \neq 15$ or 21. Then there exist odd integers r and s such that $|p^r - q^s| = 16$.*

Proof. Following the notation of Lemma 3.2, we have $\Delta = \alpha^2 \beta^2 (16\alpha - \beta)^2$ for some odd integers α and β, coprime to each other. Assume that $\alpha^2 \neq 1$; then $|\alpha| = p^r$, q^s, or $p^r q^s$. In the last case, $\beta^2 = (16\alpha - \beta)^2 = 1$, which is not possible. Therefore assume without loss of generality that $\alpha = \pm p^r$. If $\beta = \pm q^s$, $16\alpha - \beta = \pm 1$, which leads to the Diophantine equation $\pm 16 p^r - \pm q^s = \pm 1$. We get the same Diophantine equation if $\beta = \pm 1$. Therefore, we need to solve the Diophantine equation

$$q^s - 16 p^r = \pm 1.$$

Since $q^s \equiv 3 \pmod 8$ for all odd s and $q^s \equiv 1 \pmod{16}$ for all even s, we conclude that s is even and

$$q^s - 16 p^r = 1.$$

This leads to $(q^{s/2} - 1)(q^{s/2} + 1) = 16 p^r$, and since $(q^{s/2} - 1, q^{s/2} + 1) = 2$, $q^{s/2} = 7$ or 9. Therefore $q^s = 81$, which forces $p = 5$. This is not congruent to $3 \pmod 8$, so we get that $\alpha = \pm 1$.

If $\beta^2 = 1$, then $|\pm 16 - \beta|$ is 15 or 17, which again contradicts $p, q \equiv 3 \pmod 8$. We get the same result if $(\pm 16 - \beta)^2 = 1$. Therefore, $\beta = \pm p^r$ and $\pm 16 - \beta = \pm q^s$. This leads to the Diophantine equation $|p^r - q^s| = 16$. Since $p, q \equiv 3 \pmod 8$, $r \equiv s \pmod 2$. If they are both even, then the difference of the two squares equals 16, which forces $N = 15$. Therefore, r and s are odd, which is the desired result. Finally note that in this case the elliptic curve has the model

$$E : y^2 + xy = x^3 + \frac{15 + p^r}{4} x^2 + p^r x. \qquad\qquad\square$$

Theorem 3.7. *Let E be an elliptic curve with conductor pq and odd congruence number. Then $L(E, 1) \neq 0$; hence E has rank 0.*

Proof. For $pq = 15$ or 21 we can check that E has Mordell–Weil rank 0. Therefore assume that $pq \neq 15$ or 21. Recall that in Corollary 2.14 we showed that

$$u = \frac{(p-1)(q^2-1)}{48}(P_1 - P_p) \quad \text{and} \quad u' = \frac{(q-1)(p^2-1)}{48}(P_1 - P_q)$$

have order two, and $\phi(u)$ and $\phi(u')$ are linearly independent, hence they generate $E[2]$. However, since $p, q \equiv 3 \pmod 8$ we get that u and u' are odd multiples of $P_1 - P_p$ and $P_1 - P_q$, respectively. So $\pi(P_p)$ and $\pi(P_q)$ also generate $E[2]$. Therefore, $\phi(P_p - P_q)$ is nontrivial. Applying the Atkin–Lehner involution w_p to $P_p - P_q$, we get that $\phi(P_1 - P_{pq})$ is nontrivial. Therefore, $\pi(P_{pq}) \neq 0$, which implies that $L(E, 1) \neq 0$. $\qquad \square$

Level $N = 2p$. Now we take the case when $N = 2p$, for p an odd prime. Specifically, we want to show that $L(E, 1) \neq 0$. In this case it seems more straightforward to prove this using analytic tools.

Specifically, let $f_E(q) = \sum a_n q^n$ be the modular form attached to the elliptic curve E, and let Ω_E be the real period of E. Note that $L(f_E, 1) \in \mathbb{R}$ since the Fourier coefficients of f_E are rational integers. Therefore, the order of $\pi(P_{2p})$ is the order of $L(f_E, 1) \in \mathbb{R}/\Omega_E \mathbb{Z}$. We know that $L(f_E, s)$ has an Euler product expansion

$$L(f_E, s) = \prod_p L_p(f_E, s),$$

and $L_2(f_E, s) = \dfrac{1}{1 - a_2 2^{-s}}$. Similarly

$$\pi(P_p) = 2\pi i \int_{\frac{1}{2}}^{i\infty} f_E(z)\,dz = 2\pi i \int_0^{i\infty} f_E(z+1/2)\,dz = 2\pi i \int_0^{i\infty} \sum (-1)^n a_n q^n\,dz,$$

which implies that $\pi(P_p)$ can be written as $L(g, 1)$ where $L(g, s)$ has an Euler product expansion

$$L(g, s) = \left(-1 + \frac{a_2}{2^s} + \frac{a_4}{4^s} + \dots\right) \prod_{p>2} L_p(f_E, s) = -\frac{1 - a_2 2^{1-s}}{1 - a_2 2^{-s}} \prod_{p>2} L_p(f_E, s).$$

Therefore $L(g, 1) = L(f_E, 1)(a_2 - 1)$, and more appropriately for us

$$\pi(P_p) \equiv (a_2 - 1)\pi(P_{2p}) \pmod{\Omega_E \mathbb{Z}}.$$

We know that if E has odd congruence number, then $(w_2)_*$ is acting trivially, which implies that $a_2 = -1$. Therefore

$$\pi(P_p) \equiv -2\pi(P_{2p}) \pmod{\Omega_E \mathbb{Z}}.$$

However, we also know that $P_{2p} = w_2(P_p)$, and $\pi(w_2(P_p)) = \pi(P_p) + \alpha$ where α is a 2-torsion point in E. Since both $\pi(P_p)$ and $\pi(P_{2p})$ are equivalent to real numbers, α is also equivalent to a real number, which implies that $\alpha \equiv \Omega_E/2 \pmod{\Omega_E\mathbb{Z}}$. As a result we obtain successively

$$\pi(P_p) \equiv \pi(P_{2p}) + \Omega_E/2 \pmod{\Omega_E\mathbb{Z}},$$
$$-2\pi(P_{2p}) \equiv \pi(P_{2p}) + \Omega_E/2 \pmod{\Omega_E\mathbb{Z}},$$
$$-3\pi(P_{2p}) \equiv \Omega_E/2 \qquad\quad \pmod{\Omega_E\mathbb{Z}},$$
$$\pi(P_{2p}) \equiv \Omega_E\left(\tfrac{1}{3}k - \tfrac{1}{6}\right) \qquad \pmod{\Omega_E\mathbb{Z}},$$

for some integer k. Therefore, $\pi(P_{2p}) \neq 0$ and $L(f_E, 1) \neq 0$. We also observe that $\pi(P_{2p})$ will either be a 6-torsion point (for $k \equiv 0$ or $1 \pmod 3$), or a 2-torsion point (for $k \equiv 2 \pmod 3$).

In either case, we have an elliptic curve with conductor $2p$ and a rational 2-torsion point. Such elliptic curves were studied in [Ivorra 2004], whose results allow us to put stringent conditions on the values for p. Ivorra's Theorem 1 says that if $p \geq 29$, there is an integer $k \geq 4$ such that one of $p+2^k$, $p-2^k$, or $2^k - p$ is a perfect square. However, we already know from Theorem 2.15 that $p \equiv 7 \pmod{16}$. Putting these two facts together, we get that $p = 2^k - m^2$. In fact, in this case, Ivorra's result says that $7 \leq k$ is odd and our elliptic curve is isogenous to

$$y^2 + xy = x^3 + \frac{m-1}{4}x^2 + 2^{k-6}x.$$

Searching through Cremona's database, we find out that the only elliptic curves with odd modular degrees and conductors $2p$ with $p \leq 29$ are $E = 14A$ and $E = 46A$, and both of these are of the form above.

Level $N = 4p$. As with the case of $N = 2p$, we can use Theorem 2 of [Ivorra 2004] to parametrize all elliptic curves with conductor $4p$ and a rational 2-torsion point. Specifically, for $p > 29$, $p = a^2 + 4$ for some integer $a \equiv 1 \pmod 4$, and E is isomorphic to one of the following two isogenous elliptic curves:

$$E : y^2 = x^3 + ax^2 - x, \quad E' : y^2 = x^3 - 2ax^2 + px.$$

We can calculate the rank of such elliptic curves using a standard 2-descent. In fact, if we let $\phi : E \to E'$ and ϕ' be the dual isogeny, using notation from [Silverman 1992] we get

$$|S^\phi(E, \mathbb{Q})| = |S^{\phi'}(E, \mathbb{Q})| = 2,$$

which implies that

$$|E(\mathbb{Q})/\phi'(E'(\mathbb{Q}))| = |E'(\mathbb{Q})/\phi(E(\mathbb{Q}))| = 2,$$

which, by the exact sequence

$$0 \to E'(\mathbb{Q})[\phi']/\phi(E(\mathbb{Q}))[2] \to E(\mathbb{Q})/\phi'(E'(\mathbb{Q}))$$
$$\to E(\mathbb{Q})/2E(\mathbb{Q}) \to E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \to 0,$$

gives us $|E(\mathbb{Q})/2E(\mathbb{Q})| \leq 4$. This forces the rank of $E(\mathbb{Q})$ to be 0.

For $p \leq 29$, we can consult Cremona's table to get the elliptic curves $20A$, $52C$, and $116C$. In fact all these elliptic curves are of the model constructed above.

Level $N = 8p$. In this case, Theorem 3 of [Ivorra 2004] tells us that any elliptic curve with a rational 2-torsion point and the conductor $N = 8p$ satisfies $p \equiv a^2$ (mod 16) for $p > 31$. However, by Theorem 2.15, $p \equiv 3$ (mod 4); therefore there are no elliptic curves with conductor $8p$ and odd congruence number for $p > 31$. Using Cremona's table, we know that the elliptic curve $24A$ is the only elliptic curve with the conductor $8p$ and odd congruence number. Furthermore this curve has rank 0.

We combine all of the results above:

Theorem 3.8. *Let $E/\mathbb{Q}$ be an elliptic curve with odd congruence number. Then one of the following is true*:

(1) *E has conductor p and no 2-torsion point, E has supersingular reduction at 2, and $E(\mathbb{R})$ is connected.*

(2) *E has conductor p, a rational 2-torsion point, and $p = u^2 + 64$ with $u \equiv 3$ (mod 8) (E is a Neumann–Setzer curve in this case).*

(3) *E has conductor $2p$ and $p = 2^k - m^2$ for some odd integer $7 \leq k$ and integer m, and E is isogenous to*

$$y^2 + xy = x^3 + \frac{m-1}{4}x^2 + 2^{k-6}x.$$

(4) *E has conductor $4p$ and $p = m^2 + 4$ for some integer $m \equiv 1$ (mod 4), and E is isogenous to*

$$y^2 = x^3 + mx^2 - x.$$

(5) *E has conductor pq with p and q odd primes satisfying $p \equiv q \equiv 3$ (mod 8) and $p^r - q^s = 16$ for odd integers r and s, and E is isogenous to*

$$y^2 + xy = x^3 + \frac{p^r + 15}{4}x^2 + p^r x.$$

(6) *E is one of the exceptional curves $11A$, $15A$, $17A$, $19A$, $21A$, $24A$, $27A$, $32A$, $36A$, $37B$, $49A$, $243B$.*

In all these cases, E has rank 0, except possibly in case (1). In this case, we know that E has an even analytic rank.

All the curves in case (6) in the theorem have a nontrivial torsion point. Therefore we have proved that if E has odd congruence number and has a nontrivial torsion point, it has rank 0. Also note that for all the cases above, except for (1), we construct a family of elliptic curves with all the desired torsion structures and conductors. We expect that all these elliptic curves have odd congruence number. This can be proved if, for example, we show that $J_0(N)[\mathfrak{m}] \to E[2]$ is injective and $J[\mathfrak{m}] = C_N[\mathfrak{m}]$. When E is a Neumann–Setzer curve, the results of [Mazur 1977; Mestre and Oesterlé 1989] prove this result. We expect that similar results are true for the other cases; however we, do not yet know of a proof.

Acknowledgements

References

[Agashe et al. 2008] A. Agashe, K. A. Ribet, and W. A. Stein, "The modular degree, congruence primes, and multiplicity one", preprint, 2008, available at http://modular.math.washington.edu/papers/ars-congruence/.

[Breuil et al. 2001] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, "On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises", *J. Amer. Math. Soc.* **14**:4 (2001), 843–939. MR 2002d:11058 Zbl 0982.11033

[Calegari and Emerton 2009] F. Calegari and M. Emerton, "Elliptic curves of odd modular degree", *Israel J. Math.* **169** (2009), 417–444. MR 2010k:11092 Zbl 05508747

[Chua and Ling 1997] S.-K. Chua and S. Ling, "On the rational cuspidal subgroup and the rational torsion points of $J_0(pq)$", *Proc. Amer. Math. Soc.* **125**:8 (1997), 2255–2263. MR 98f:11065 Zbl 0891.11036

[Cremona] J. Cremona, "Elliptic curve data", database, available at http://www.warwick.ac.uk/staff/J.E.Cremona/ftp/data/INDEX.html.

[Dummigan 2006] N. Dummigan, "On a conjecture of Watkins", *J. Théor. Nombres Bordeaux* **18**:2 (2006), 345–355. MR 2007j:11072 Zbl 1161.11351

[Emerton 2003] M. Emerton, "Optimal quotients of modular Jacobians", *Math. Ann.* **327**:3 (2003), 429–458. MR 2005g:11100 Zbl 1061.11018

[Frey 1997] G. Frey, "On ternary equations of Fermat type and relations with elliptic curves", pp. 527–548 in *Modular forms and Fermat's last theorem* (Boston, 1995), edited by G. Cornell et al., Springer, New York, 1997. MR 1638494 Zbl 0976.11027

[Gross and Zagier 1986] B. H. Gross and D. B. Zagier, "Heegner points and derivatives of L-series", *Invent. Math.* **84**:2 (1986), 225–320. MR 87j:11057 Zbl 0608.14019

[Ivorra 2004] W. Ivorra, "Courbes elliptiques sur $\mathbb{Q}$, ayant un point d'ordre 2 rationnel sur $\mathbb{Q}$, de conducteur $2^N p$", *Dissertationes Math.* (*Rozprawy Mat.*) **429** (2004), 1–55. MR 2006h:11056 Zbl 1076.11037

[Kolyvagin 1988] 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**:3 (1988), 522–540, 670–671. In Russian; translated in *Math. USSR, Izv.* **32**:3 (1989), 523–541. MR 89m:11056

[Ligozat 1975] G. Ligozat, *Courbes modulaires de genre* 1, Mem. Soc. Math. de France (old ser.) **43**, Société Mathématique de France, Paris, 1975. MR 54 #5121 Zbl 0322.14011

[Ling 1997] S. Ling, "On the $\mathbb{Q}$-rational cuspidal subgroup and the component group of $J_0(p^r)$", *Israel J. Math.* **99** (1997), 29–54. MR 98e:11076 Zbl 0934.14022

[Mazur 1977] B. Mazur, "Modular curves and the Eisenstein ideal", *Inst. Hautes Études Sci. Publ. Math.* **47** (1977), 33–186. MR 80c:14015 Zbl 0394.14008

[Mestre and Oesterlé 1989] J.-F. Mestre and J. Oesterlé, "Courbes de Weil semi-stables de discriminant une puissance m-ième", *J. Reine Angew. Math.* **400** (1989), 173–184. MR 90g:11078 Zbl 0693.14004

[Murty 1999] M. R. Murty, "Bounds for congruence primes", pp. 177–192 in *Automorphic forms, automorphic representations, and arithmetic* (Fort Worth, TX, 1996), Proc. Sympos. Pure Math. **66**, Amer. Math. Soc., Providence, RI, 1999. MR 2000g:11038 Zbl 0933.11024

[Ogg 1974] A. P. Ogg, "Hyperelliptic modular curves", *Bull. Soc. Math. France* **102** (1974), 449–462. MR 51 #514 Zbl 0314.10018

[Ribet 1980] K. A. Ribet, "Twists of modular forms and endomorphisms of abelian varieties", *Math. Ann.* **253**:1 (1980), 43–62. MR 82e:10043 Zbl 0421.14008

[Ribet 1981] K. A. Ribet, "Endomorphism algebras of abelian varieties attached to newforms of weight 2", pp. 263–276 in *Seminaire de Théorie de Nombres* (Paris, 1979–80), edited by M.-J. Bertin, Progr. Math. **12**, Birkhäuser, Boston, 1981. MR 82m:10044 Zbl 0467.14006

[Shimura 1971] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publ. Math. Soc. Japan **11**, Princeton Univ. Press, Princeton, NJ, 1971. MR 47 #3318 Zbl 0872.11023

[Silverman 1992] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer, New York, 1992. MR 95m:11054

[Stein and Watkins 2002] W. A. Stein and M. Watkins, "A database of elliptic curves: first report", pp. 267–275 in *Algorithmic number theory* (Sydney, 2002), Lecture Notes in Comput. Sci. **2369**, Springer, Berlin, 2002. MR 2005h:11113 Zbl 1058.11036

[Stein and Watkins 2004] W. Stein and M. Watkins, "Modular parametrizations of Neumann–Setzer elliptic curves", *Int. Math. Res. Not.* **2004**:27 (2004), 1395–1405. MR 2005c:11070 Zbl 1088.11043

[Taylor and Wiles 1995] R. Taylor and A. Wiles, "Ring-theoretic properties of certain Hecke algebras", *Ann. of Math.* (2) **141**:3 (1995), 553–572. MR 96d:11072 Zbl 0823.11030

[Watkins 2002] M. Watkins, "Computing the modular degree of an elliptic curve", *Experiment. Math.* **11**:4 (2002), 487–502. MR 2004c:11091 Zbl 1162.11349

[Wiles 1995] A. Wiles, "Modular elliptic curves and Fermat's last theorem", *Ann. of Math.* (2) **141**:3 (1995), 443–551. MR 96d:11071 Zbl 0823.11029

syazdani@math.mcmaster.ca   *Department of Mathematics and Statistics,*
                               McMaster University, Hamilton, ON L8S 4L8, Canada

Algebra & Number Theory

www.jant.org

See inside back cover or www.jant.org for submission instructions.

Algebra & Number Theory