MODULAR ABELIAN VARIETIES OF ODD MODULAR DEGREES

S. YAZDANI

Abstract. In this paper, we will study modular Abelian varieties with odd congruence numbers by examining the cuspidal subgroup of $J_0(N)$. We will 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 an odd congruence number, then $N$ has at most two prime divisors, and if $N$ is odd, then $N = p^a$ or $N = pq$ for some prime $p$ and $q$. In the second half of this paper, we will focus on modular elliptic curves with odd modular degree. Our results, combined with the work of Agashe, Ribet, and Stein, finds necessary condition for elliptic curves to have odd modular degree. In the process we prove Watkins's 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 the work of Wiles, Taylor-Wiles, et al, we know that $E$ is modular (see [2]), 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 $\pi$, which we call the modular degree of $E$. This invariant is related to many other invariants of an the elliptic curve. For instance, this number is closely related to the congruences between $E$ and other modular forms (see 1.1 and [1]). Also, we know that finding a good bound on the degree of $\pi$ in terms of $N$ is equivalent to the $ABC$ conjecture (see [16], [8]).

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 [24]). In the particular case when the modular degree of $E$ is odd, Watkins’s conjecture implies $E(\mathbb{Q})$ is finite. Searching through Cremona, Stein, and Watkins’s database ([22] and [1]) for elliptic curves of odd modular degree, Calegari and Emerton 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 [23] and [3]). Dummigan has recently provided a heuristic explanation for Watkins’s conjecture. His method uses the Selmer group of the symmetric square of $E$ and its relationship to congruences between modular forms (see [6]).

The goal of this paper is to generalize the results of Calegari and Emerton to modular Abelian varieties having odd modular exponents and odd congruence number (see [1] for definition). We find necessary conditions for a modular Abelian variety to have an odd congruence number. Specifically in theorem 2.15 we show that if a modular Abelian variety with conductor $N$ has an 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.

This research was partially supported by NSERC.
In section 3 we study elliptic curves having odd congruence numbers. Recall that the result of Agashe, Ribet, and Stein, states 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). We find more stringent conditions that elliptic curves with an odd congruence number need to satisfy. Specifically if an elliptic curve $E$ with conductor $N$ has an 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 non-trivial 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 of this article. In section 1 we review some of the definitions used in this paper, along with some results that come in handy in the rest of the paper. Specifically, in section 1.2 we recall how to calculate the rational cuspidal subgroup of $J_0(N)$, and in section 1.3 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 numbers, 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 non prime-power conductor and if $A$ has an odd congruence number, then it must have a rational 2-torsion point (theorem 2.1). We also show that if $A$ has an odd congruence number and a rational 2-torsion point, then all of the new rational 2-torsion points of $J_0(N)$ map injectively to $A$ (see section 2.3). We use this fact and our analysis of cuspidal subgroup to show that if $A$ has an 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 complex multiplication or an inner twist (section 2.2). In section 3 we apply our results to elliptic curves. Theorem 2.15 gives us different type of conductors that elliptic curves with odd congruence number must satisfy. In each subsection of section 3 we study one of these cases, and 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).

Acknowledgements: This paper would not have been possible without the help of my advisor, Ken Ribet. Specifically, many of the results in section 2.4 were suggested to me by him. I would also like to thank Frank Calegari, Matt Emerton, William Stein, and Jared Weinstein, with whom I have had many discussions. Manfred Kolster and Romyar Sharifi gave me very useful feedback on the first draft of this article. Finally, I would like to thank Jovanca Buac for her careful reading of this paper and all of her suggestions.

1. Preliminaries

Let $N$ be a positive integer and $X_0(N)$ be the moduli space of elliptic curves with a cyclic subgroup of order $N$. Let $C_N \subset X_0(N)$ be the set of cusps of $X_0(N)$, that is $C_N = \pi^{-1}(\infty)$, where $\pi : X_0(N) \to X_0(1)$ is the natural degeneracy map.

Footnote: In fact, by searching through Cremona table of elliptic curve, it seems that an elliptic curve has an odd congruence number if and only if it has an odd modular degree.
and \( \infty \) is the unique cusp on \( X_0(1) \). All such cusps can be represented as rational numbers \( \frac{a}{b} \in \mathbb{H} \), with \( a \) and \( b \) positive coprime integers and \( b|N \). Furthermore, there is a unique representative for any cusp with \( a \leq (b, N/b) \). Under this representation, \( \infty = \frac{1}{N} \). For any integer \( r|N \) such that \( \gcd(r, N/r) = 1 \), we can define the Atkin-Lehner involution \( w_r : X_0(N) \to X_0(N) \), by sending \( (E, D) \in X_0(N) \) to \( (E/D[r], (E[r] + D)/D[r])^2 \). We usually abuse notation by letting \( w_T = w_r \) whenever \( T = \prod_{l|\tau} l \) (for example \( w_4 = w_2 \) on \( X_0(4N) \)).

Let \( S(N) \) be the space of weight two cuspidal \( \mathbb{Z} \)-forms on \( \Gamma_0(N) \). Let \( \mathbb{T} \) denote the \( \mathbb{Z} \)-algebra of the Hecke operators acting on \( S(N) \). As usual, we denote \( J_0(N) = \text{Jac}(X_0(N)) \). 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 \( i(z) = (z) - (\infty) \).

Let that for any map \( w : X_0(N) \to X_0(N) \) we have the induced map
\[
w_\ast : J_0(N) \to J_0(N) \quad \sum(z) \mapsto \sum(w(z)).
\]

1.1. 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 \( \phi' : A' \to J_0(N)' \). Since \( J_0(N) \) is self dual, we can compose these two morphisms to get
\[
\psi : A' \to A.
\]

Following [1], define modular number to be the order of \( \ker(\psi) \), and modular exponent to be its exponent, denoted by \( \tilde{n}_A \). If \( A \) is an elliptic curve, then \( \tilde{n}_A \) equals to 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 \( \tilde{r}_A \) (see lemma 4.3 of [1]). Let \( m \subset \mathbb{T} \) be a maximal ideal of \( \mathbb{T} \). Then \( A[m] \neq 0 \) (resp. \( B[m] \neq 0 \)) if and only if image of \( m \) in \( \mathbb{T}_A \) (resp. \( \mathbb{T}_B \)) is a proper maximal ideal. If \( A[m] \) and \( B[m] \) are both nontrivial, then by tensoring \( \mathbb{T} \to \mathbb{T}_A \oplus \mathbb{T}_B \) by \( \mathbb{T}/m \), we see that the cokernel is a nontrivial vector space over \( \mathbb{T}/m \), which means that the characteristic of \( \mathbb{T}/m \) divides the congruence exponent of \( A \). On the other hand, if \( A[m] \neq 0 \), then \( A'[m] \neq 0 \), and if \( A[m] \cap B[m] \neq 0 \), then the characteristic of \( \mathbb{T}/m \) divides the modular exponent.

In [1], 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

\[\text{As usual, } G[r] \text{ is the set of } r\text{-torsion points of the group } G.\]
(1) $\widetilde{n}_{A_f} | \widetilde{r}_{A_f}$, and
(2) if $p^2 \mid N$, then $\text{ord}_p(\widetilde{n}_{A_f}) = \text{ord}_p(\widetilde{r}_{A_f})$.

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.

1.2. Cuspidal Subgroup. The cuspidal subgroup of $J_0(N)$ is the subgroup generated 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 is studied for $N$ a power of a prime by San Ling [13] and for $N$ the product of the two primes by Seng-Kiat Chua and San Ling [4]. Following [13], let

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

With this notation we get

**Proposition 1.2.** The rational cuspidal subgroup $C_N \subset J_0(N)$ is generated by the elements $\phi(\gcd(d,N/d))(P_d - P_1)$, where $\phi(k)$ is the Euler $\phi$-function.

*Proof.* See [13]. \qed

In this subsection, we calculate the order of certain elements in this group. Recall that Dedekind’s eta function is defined as

$$\eta(\tau) = q^{1/24} \prod_{n=1}^{\infty} (1 - q^n),$$

where $q = e^{2\pi i \tau}$. Let $\eta(M\tau) = \eta_M(\tau)$. We use $\eta_M$ to construct functions with divisors supported on the cusps. In particular, for $M|N$, $\eta_M$ has a zero of order

$$(1) \quad \frac{1}{d} \frac{N d'^2}{24 \text{d}^2 M},$$

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, [17]). The following result of Ligozat can be used to calculate the order of specific cusps.

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

1. All of the rational numbers $r_\delta$, are rational integers;
2. $\sum_{\delta|N} r_\delta \delta \equiv 0 \pmod{24}$;
3. $\sum_{\delta|N} r_\delta \delta \phi(\delta) \equiv 0 \pmod{24}$;
4. $\sum_{\delta|N} r_\delta = 0$;
5. $\prod_{\delta|N} \delta^{x_\delta}$ is a square of a rational number.

*Proof.* See [12]. \qed

---

---

3Our notation is slightly different from San Ling’s papers. Specifically San Ling’s $P_d$ is $\gcd(d,N/d)$ times our $P_d$.

4This is the only section where $\phi$ is the Euler function. For the rest of the paper, whenever results of this section are used, $\phi(\gcd(d,N/d)) = 1$. Also outside of this section, $\phi$ is reserved for the map $\phi : J_0(N) \to A$. 

---
We also know that the lattice of divisors linearly equivalent to zero supported on the cusps is generated by the divisors of $g_r$ that are modular functions. Let $N = \prod_{i=1}^{k} p_i^{n_i}$ 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 $P_{\prod p_i^{s_i}} \rightarrow \bigotimes_i P_{p_i^{s_i}}$.) Similarly, let $W$ be rational vector space of functions $g_r$ (as defined in proposition 13) under multiplication. Then we have $W \cong \bigotimes_i W_{p_i}$ 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 $\Lambda : V \rightarrow W$ where $\Lambda^{-1}(g)$ is the divisor attached to $g$. We can verify that this isomorphism can be written very explicitly as

$$24 \bigotimes_{p_i} \Lambda_{p_i},$$

where $\Lambda_{p_i} : V_{p_i} \rightarrow W_{p_i}$ and $\Lambda_{p_i}$ is the tridiagonal matrix (under the above basis)

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

Note that when $f \in W$ is a modular function, $\Lambda^{-1}(f)$ is linearly equivalent to zero. Therefore, by combining proposition 13 and the above isomorphism we get

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

1. All of the coefficients in $\Lambda v$ are integral;
2. $v$ has degree 0;
3. $v$ is integral and the coefficient of $P_d$ divides $\phi(d, N/d)$;
4. Let $e_i = (1, 1, 1, \ldots, 1) \in W_{p_i^{s_i}}$ and $f_i = (0, 1, 0, 1, \ldots) \in W_{p_i^{s_i}}$. Then for each $i$,

$$(e_1 \otimes \cdots \otimes f_i \otimes \cdots \otimes e_k) \Lambda v$$

is an even number.

**Proof.** This is a straightforward rewording of proposition 13. \qed

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 square free odd integer and $s_2 < 4$ (the case we come across in this paper), then condition three is reduced to the coefficients of $v$ being integral. Therefore, the denominator of $\Lambda(v)$ gives the order of $v$ or half of the order of $v$.

We use the above proposition to calculate the order of various cusps:
On the other hand, \( n \) is even, which implies that \( N \) of the work of Ogg [17] in the case where \( p \) is odd. This is a generalization of the work of Ogg [17] in the case where \( N = pq \). Note that

\[
\Lambda z = \frac{24}{\prod_i (p_i^2 - 1)(p_i - 1)} \left( \bigotimes_i \begin{pmatrix} p_i(p_i - 1) & -(p_i - 1) \\ -(p_i - 1) & p_i(p_i - 1) \end{pmatrix} \begin{pmatrix} 1 \\ b_i \end{pmatrix} \right) = \frac{24}{\prod_i (p_i^2 - 1)} \left( \bigotimes_i \begin{pmatrix} p_i - b_i \\ (p_i - b_i)b_i \end{pmatrix} \right) = \frac{24}{\prod_i (p_i + b_i)} \left( \bigotimes_i \begin{pmatrix} 1 \\ b_i \end{pmatrix} \right).
\]

Considering the coefficient of the first coordinate, the order is at least \( n = \text{Num} \left( \prod_i (p_i + b_i)/24 \right) \). On the other hand, \( n\Lambda z = \bigotimes_i \begin{pmatrix} 1 \\ b_i \end{pmatrix} \). Therefore

\[
(e_1 \otimes \cdots \otimes f_i \otimes \cdots \otimes e_t)(n\Lambda z),
\]

is even, which implies that \( n\Lambda z \) is trivial. Therefore the order of \( z \) is

\[
\text{Num} \left( \frac{\prod_i (p_i + b_i)}{24} \right).
\]

### 1.3. Hecke Action

In this section we recall the explicit action of the Hecke operators \( T_i \) 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 \( p|N \) and \( V = \bigotimes V_{p_i} \). Then \( T_p \) acts trivially on \( V_{p_i} \) for \( p_i \neq p \), and as

\[
\begin{pmatrix}
1 & 0 & \cdots & 0 & 0 \\
p - 1 & 0 & \cdots & 0 & 0 \\
0 & p & \cdots & 0 & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \cdots & 0 & 0 \\
0 & 0 & \cdots & p & p
\end{pmatrix}
\]
Calculating the action of various Hecke operators on the above elements is a straightforward matrix multiplication. As for proving $T$-congruences between modular forms in later sections.

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 $T_p$ for 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 $v = \bigotimes v_i$ be an element in the cuspidal subgroup. Then

1. If $p||N$ and $v_p = P_1 - P_p$ then $T_p v = v$.
2. If $p\!\not|\!N$ and $v_p = P_1 + P_p$ then $T_p v = v + 2u$ where $u = \bigotimes u_l$ with $u_l = v_l$ for all $l \neq p$ and $v_p = (p - 1)P_p$.
3. If $N = 4M$ and $v_2 = P_2$ then $T_2 v = u$ with $u = \bigotimes u_l$ with $u_l = v_l$ for all odd $l$.
4. If $N = 8M$ and $v_2 = P_1 - P_8$ then $T_2 v = u$ where $u = \bigotimes u_l$ with $u_2 = P_1 + P_2 - 2P_4$ and $u_l = v_l$ for all odd $l$.

Specifically, in all of the cases above, if $\lambda v$ is of order 2 for some integer $\lambda$, then $T_p(\lambda v) = \lambda v$ for all odd $p|N$ and $T_2(\lambda v) = \lambda v$ (resp. $T_2(\lambda v) = 0$) when $N = 2M$ (resp. $N = 4M$ or $N = 8M$).

**Proof.** Calculating the action of various Hecke operators on the above elements is a straightforward matrix multiplication. As for proving $T_p(\lambda v) = \lambda v$ when $N$ is square free, case one follows by definition. In second case (when $v_p = P_1 + P_p$), we can verify that $u$ has the same order as $v$, hence $2\lambda u = 0$. As for the cases $N = 4M$ or $N = 8M$, we can check that order of $T_2 v$ is half of the order $v$, hence $T_2(\lambda v) = 0$. \hfill $\Box$

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 above proposition is finding explicit 2-torsion points of $C_N$ that are 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 numbers. 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 an 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 \( \phi \). As usual, let \( \mathcal{T} \) be the Hecke algebra acting on \( J_0(N) \) and \( S(N) \).

2.1. 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 an odd modular exponent. Then if \( A(\mathbb{Q}) \) has no 2-torsion points, then 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, then the conductor of \( A \) is a power of a prime.

This theorem was proved by Calegari and Emerton in the case where \( A \) is an elliptic curve (theorem 2.1 of [3]). Here, we apply their techniques to higher dimensional modular Abelian varieties. We must prove a few lemmata first.

**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

\[
\text{Jac}(Y) \simeq \text{Jac}(Y)^\vee \xrightarrow{f^*} \text{Jac}(X)^\vee \simeq \text{Jac}(X) \xrightarrow{f_*} \text{Jac}(Y)
\]

is multiplication by \( m \).

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

\[
f_*[f^*((z_1) - (z_2))] = f_* \left( \sum_{f(y_1) = z_1} (y_1) - \sum_{f(y_2) = z_2} (y_2) \right)
\]

\[
= \left( \sum_{y_1 \in f^{-1}(z_1)} (z_1) - \sum_{y_2 = f^{-1}(z_2)} (z_2) \right)
\]

\[
= m((z_1) - (z_2))
\]

where the summations are understood to account for multiplicities. \( \Box \)

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

\[
\begin{diagram}
X_0(N) \rto^\pi \atop \rtwocell{w} \downarrow \rto_{\pi} & A \\
X_0(N) \rto_{\pi} \atop \rtwocell{w} \downarrow & X_0(N)/w \rto & A
\end{diagram}
\]

commutes. Then the modular exponent of \( A \) is even.

**Proof.** The above assumptions imply that \( \pi \) factors through

\[
X_0(N) \rto \to X_0(N)/w \rto A.
\]
Therefore \( \phi \) factors through
\[
\text{Jac}(X_0(N)) \longrightarrow \text{Jac}(X_0(N)/w) \longrightarrow A.
\]
Dualizing the above diagram and using the autoduality of \( J_0(N) \), we get
\[
\text{Jac}(X_0(N)/w)^{\vee} \longrightarrow J_0(N)^{\vee}
\]
\[
A \quad \text{Jac}(X_0(N)/w) \quad J_0(N)
\]
By lemma 2.2 the middle arrow is multiplication by 2, since the degree of \( X_0(N) \rightarrow X_0(N)/w \) is 2. Using the commutativity of the above diagram, we can see that \( A^{\vee}[2] \subset \ker(\delta) \). Recalling that the modular exponent is the exponent of the kernel of \( \delta \), we conclude that the modular exponent of \( A \) is even.

Recall that for an involution map \( w : X_0(N) \rightarrow X_0(N) \), we get the induced map \( w_* : J_0(N) \rightarrow J_0(N) \). Let \( A \) be an optimal modular Abelian variety, and \( \phi : J_0(N) \rightarrow A \) 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 an odd modular exponent. As before let \( \pi : X_0(N) \rightarrow A \) be the composition of Albanese embedding \( X_0(N) \rightarrow J_0(N) \) and \( \phi \). Assume that for some involution \( w, w_* : J_0(N) \rightarrow J_0(N) \) descends down to a trivial action on \( A \). Then \( \pi(w(z)) - \pi(z) \) is a nontrivial \( k \)-rational 2-torsion point for all \( z \in X_0(N)(\mathbb{K}) \).

**Proof.** Recall that \( P_1 \) is the cusp at infinity and \( \pi(z) = \phi(z - P_1) \). Then we get
\[
\pi(w(z)) - \pi(z) = \phi(w(z) - P_1) - \phi(z - P_1)
\]
\[
= \phi(w(z) - w(P_1)) - \phi(z - P_1) + \phi(w(P_1) - P_1)
\]
\[
= w_*(\phi(z - P_1)) - \phi(z - P_1) + \phi(w(P_1) - P_1)
\]
\[
= \pi(w(P_1)).
\]
Therefore \( \pi(w(z)) = \pi(z) + \pi(w(P_1)) \) for all \( z \in X_0(N) \). Applying this equation 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 2.2 if \( A \) has an 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.

Given the above lemma, we can now prove theorem 2.1.

**Proof.** 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 \( w_*(z) = \pm z \) for all \( z \in A(\mathbb{K}) \). This gives us a map \( W \rightarrow \{\pm 1\} \). 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 non-trivial element \( w \in W_0 \), that is \( w_*(z) = z \) for all \( z \in A(\mathbb{K}) \). 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 simple modular simple Abelian variety with conductor $N$ and an odd modular exponent. If the Atkin-Lehner involution $w_r : X_0(N) \to X_0(N)$ has a fixed point then $(w_r)_\ast$ acts as $-1$ on $A$. Specifically, $(w_N)_\ast$ acts as $-1$ on $A$. When $N = 2M$ (resp. $N = 4M$), $(w_2)_\ast$ acts as 1 (resp. $(w_2)_\ast$ acts as $-1$) on $A$.

**Proof.** Let $P \in X_0(N)(\mathbb{Q})$ 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 $(w_r)_\ast = 1$ then $\pi(w_r(z)) - \pi(z) = \pi(w_r(P_1))$ for any $z \in X_0(N)(\mathbb{Q})$. Specifically, we get $\pi(w_r(z)) = \pi(z)$, which by lemma 2.3 implies that $A$ has an even congruence number. Therefore $(w_r)_\ast = -1$ 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 $\frac{1}{M-\sqrt{N}}$ is fixed under $(w_M)_\ast$. Similarly, when $N = 4M$, $P_2$ is fixed under $(w_2)_\ast$. Therefore, we have the desired result. 

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

**Corollary 2.6.** If $A$ is a simple modular Abelian variety with an odd congruence number, 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 2 prime divisors then $E$ has even modular degree.

### 2.2. Non-Semistable Case

The goal of this subsection is to prove the following

**Theorem 2.8.** Let $A$ be an absolutely simple modular Abelian variety $A$ of level $N$ with an odd congruence number. Let $\delta_p = 0$ for the odd primes $p$ and $\delta_2 = 2$. Assume that $p^{2+4s}|N$. 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 to show that such modular Abelian varieties have inner twists or complex multiplication by a character of conductor $p$ (see 3)). Using the results of Ribet on inner twists 19, 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 $\text{End}_{\mathbb{Q}}(A) \otimes \mathbb{Q}$ is a matrix algebra, then $A$ is not absolutely simple.

**Proof.** Assume that $R = \text{End}_{\mathbb{Q}}(A) \otimes \mathbb{Q}$ is a matrix algebra. We can find the projections $e_1, e_2 \in R$ such that $e_1 + e_2 = \text{Id}$, $e_1e_2 = 0$, and $e_1, e_2 \notin \{0, \text{Id}\}$. For
some integer \( n \), \( ne_i \in \End_A(A) \). If we assume that \( A \) is absolutely simple, the image of \( ne_i A \) must be \( A \) or \( 0 \). However, since \( (ne_1)(ne_2) = n^2e_1e_2 \neq 0 \), one of them must be \( 0 \). Assume without loss of generality that \( ne_2 = 0 \) in \( \End_Q(A) \). This implies that \( e_2 = 0 \), which contradicts our assumption that \( e_2 \notin \{0, \text{Id} \} \). Therefore, \( A \) is not absolutely simple.

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 \( f = \sum a_nq^n \) be one such eigenform, and \( E = \mathbb{Q}(a_n) \) be the field of definition of \( f \). We know that \( \End_Q(A) \otimes \mathbb{Q} = E \). Let \( D = \End_Q(A) \otimes \mathbb{Q} \) be the algebra of all of the endomorphisms of \( A \). From [18] 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 an odd congruence number. Let \( \delta_p = 0 \) for odd primes and \( \delta_p = 2 \). If \( p^{2+\delta_p}|N \) then \( A \) 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 \( f_A = \sum a_nq^n \in \mathbb{C}((q)) \) be a normalized eigenform associated with \( A \). Let \( E = \mathbb{Q}(a_n) \subset \mathbb{C} \). Let \( \chi \) 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 [20]). Since \( \chi \) is a quadratic character, \( \chi \) takes values in \( \pm 1 \), and as a result \( \chi \otimes f_A \equiv f_A \pmod{\lambda} \) for any \( \lambda | 2 \). If \( A \) has an 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 \( \chi \), 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 \( \gamma \in \Hom(E, \mathbb{C}) \). Let \( \Gamma \subset \Hom(E, \mathbb{C}) \) such that for any \( \gamma \in \Gamma \) we can find a character \( \chi_\gamma \) such that \( \chi_\gamma \otimes f_A = \gamma(f_A) \). By [19], \( F = E^\Gamma \) and (as discussed above) \( D = \End_Q(A) \otimes \mathbb{Q} \) must be a quaternion algebra. However, using theorem 3 of [18], \( A \) has potentially good reduction everywhere, as desired.

The final claim of the lemma follows by noting that if \( q|N \) but \( q^2 \not| N \), then \( A \) has multiplicative reduction over any field extension. 

We now proceed to prove 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 \( \Gamma \subset \Hom(E, \mathbb{C}) \) will have at least four elements, \( \gamma_1, \gamma_p, \gamma_q, \) and \( \gamma_{pq} \). 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 \( \chi_p \) and \( \chi_q \), which is impossible. This completes the proof of the main theorem in this section.

2.3. Algebraic Congruence Number. In this section we 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 \( \phi \) is the modular uniformization map \( \phi : J_0(N) \rightarrow A \). Assume that \( N \) is not a power of a prime. Then theorem 2.8 says that \( A[2](Q) \) has a non-trivial element. Let \( z \in A[2](Q) \) be a non-trivial rational 2-torsion point of \( A \), and let \( \mathfrak{m} \subset T \) be the annihilator of \( z \). Since \( z \in A[\mathfrak{m}] \neq 0 \), we get that \( A'[\mathfrak{m}] \neq 0 \). 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 \( B[\mathfrak{m}] \neq 0 \).

We have the following lemma.

**Lemma 2.11.** Let \( A \) be a new simple modular Abelian variety, \( 0 \neq z = A[2](Q) \), and let \( \mathfrak{m} \) be the annihilator of \( z \) in \( T \). Then \( \mathfrak{m} \) is generated by 2, \( T_1 - (l + 1) \) for \( l \nmid N \), \( T_p - 1 \) for \( p \mid p^2 \nmid N \), and \( T_p \) for \( p^2 \mid N \).

**Proof.** Clearly \( z \) is killed by 2, and by the Eichler-Shimura relationship, \( T_1(z) = (\Frob_p + l/Frob_p)(z) = (l+1)z \), since \( z \) is rational. Since \( A \) is a new modular Abelian variety, if \( p \mid |N| \), we have \( T_p(z) = \pm z = z \), and if \( p^2 \mid N \) then \( T_p(z) = 0 \). This is the desired result. \( \square \)

Recall that \( C_N \subset J_0(N) \) is the rational cuspidal subgroup of \( J_0(N) \). Let \( \mathfrak{m} \subset T \) be the annihilator of \( z \in A[2] \). By definition we have that if \( B[\mathfrak{m}] \neq 0 \), then \( A \) will have an even congruence number. We can use proposition 1.7 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 such that \( \phi(v) = 0 \), then \( v \in B \cap C_N \). Now if \( \lambda v \subset C_N[\mathfrak{m}] \). Therefore, we only need to check that such \( v \)'s have even order and that \( \phi(v) = 0 \) to show that \( A \) has an even congruence number.

**Theorem 2.12.** Let \( A \) be a new absolutely simple optimal modular Abelian variety with an 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 an 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 \( M \) square free odd integer, and \( \alpha < 4 \). Furthermore, by theorem 2.8, we can find a non-trivial \( z \in A[2](Q) \). Let \( \mathfrak{m} \) be the annihilator of \( z \). We now find \( v \in C_N \) of the form considered in proposition 1.7 such that \( v \) has even order and \( \phi(v) = 0 \). We will consider three main cases, based on the valuation of \( N \) at 2.

Assume that \( 4 \nmid N \). Since \( w_N = \prod_{l \mid N} w_l \), 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 \( 2 \mid N \), 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

\[
v = (1-wqr)(1+s_pw_p)(1+s_qw_q)P_1 = (1+s_pw_p)(1+s_qw_q)(1-s_qw_r)P_1.
\]
By the computation from section 2.2 we get that \( v \) has order \( \text{Num} \left( \frac{(1+s_p q) (1+s_q w)}{2} \right) \).

If we select \( s_p \equiv -p \pmod{4} \) and \( s_q \equiv -q \pmod{4} \), then this order is even. Furthermore, note that \( v \) is of the form considered in proposition 1.7 so we only need to show that \( \phi(v) = 0 \) to prove \( A \) has an even congruence number. 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 
\[
\phi(v) = \phi(w_{qr}(P) - P) = \sum_{m|pq} \pi(w_{qr}(P_m)) - \pi(P_m)
\]
\[
= 4a = 0,
\]
which shows that \( A \) has an even congruence number.

Assume that \( 4||N \). By lemma 2.3 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 \( s_q = \pm 1 \). The order of \( v \) is \( \text{Num} \left( \frac{(1-p)(1+s_q w_q)}{2} \right) \).

If we select \( s_q \equiv -q \pmod{4} \), then \( v \) will have an even order. Again note that \( v \) is of the form considered in proposition 1.7. 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 
\[
v = (1 - w_2)(1 + s_p w_p)(1 + s_q w_q)P_1 = (1 - w_2)(1 + s_p w_p)(1 + s_q w_q)P_1.
\]
Then \( v \) has order \( \text{Num} \left( \frac{(1+s_p w_p)(1+s_q w_q)}{2} \right) \) that is even. Again, \( v \) is of the form considered in proposition 1.7 and 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 
\[
P = (1 - w_2)(1 \pm w').
\]
That shows \( \phi(v) = 0 \). Therefore \( A \) in this case will have an even congruence number again. \( \Box \)

Combining this result with the main result of section 2.2, we get

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

### 2.4. Congruence Classes of Primes

Let \( A \) be a simple modular Abelian variety of conductor \( N \) with an 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 \( \phi \). Assume that \( N \) is not a power of a prime, which by theorem 2.4 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 \((w_p)_*\) 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 \( \text{Num} \left( \frac{(w_p + 1)(q - 1)}{24} \right) \). Since we are assuming that \( A \) has odd congruence number, we get that \( p \equiv \pm 3 \pmod{8} \) and \( q \equiv 3 \pmod{4} \).

We record a useful corollary of the above result.

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

**Proof.** We prove this by finding two distinct points in \( C_N[m] \). First note that \( P_1 - P_p \) and \( P_1 - P_q \) have the orders \((p - 1)(q^2 - 1)/24\) and \((p^2 - 1)(q - 1)/24\), respectively. Therefore, both
\[
u = \frac{(p - 1)(q^2 - 1)}{48}(P_1 - P_p), u' = \frac{(p^2 - 1)(q - 1)}{48}(P_1 - P_q)
\]
are of order 2. We can easily check that \( T_pu = u \) and \( T_qu' = u' \). On the other hand
\[
u + T_qu = \frac{(p - 1)(q^2 - 1)}{48}(P_1 - P_p + P_q - P_{pq}),
\]
which is zero. Similarly, we get \( u' + T_pu' = 0 \). Therefore, \( u, u' \in C_N[m] \). Furthermore, we know that \( A(u + u') \) 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 \( C_N[m] \) is at least 2-dimensional over \( \mathbb{F}_2 \). Since we are assuming that \( A \) has an odd congruence number, \( C_N[m] \) 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 \( \frac{p^2 - 1}{16} \)) must have an even order. Let \( v = \frac{p^2 - 1}{16}(P_2 - P_1) \in C_N[2] \). By proposition 1.7 \( T_p(v) = T_2(v) = v \), hence \( v \in C_N[m] \). 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 \( \frac{p^2 - 1}{16} \) is even, then \( \pi(v) = 0 \). This implies that \( z \in C_N[m] \cap B \), and, in turn, that the congruence number is even. Since we are assuming that the congruence number of \( A \) is odd, we get that \( \frac{p^2 - 1}{16} \) 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 \( \pmod{p} \), 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 \((w_p)_*\) acts as \(-1\) on \( A \), while \((w_q)_*\) acts trivially. Therefore, \( \pi(P_2) - \pi(P_{pq}) = \pi(P_2) - \pi(w_p(P_2)) \in A[2] \). The order of \( P_2 - P_{pq} \) is \( \frac{p^2 - 1}{2} \). Therefore, if \( A \) has an odd congruence number, \( \frac{p - 1}{4} \) 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 \( \frac{p-1}{2} \). 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 \((w_p)_\ast\).

We combine the above results in the following theorem.

**Theorem 2.15.** Let \( A \) be a new modular Abelian variety with an 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 Numbers**

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 \( p, \, pq, \, 2p, \, 4p, \, 8p \), 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 \([1]\) that when \( 4 \nmid N \), then having an odd congruence number is the same as having odd modular degree. We conjecture that in fact having an odd congruence number is equivalent to odd modular degree in all cases. As a result, we can state many of our results in terms of modular degrees.

3.1. **Complex Multiplication.** Let \( E \) be an elliptic curve of conductor \( N \). If \( p^2 \mid N \) for an odd prime \( p \), then by section \([2]\) we know that \( E \) has complex multiplication. We also showed that if \( 16 \mid N \) 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 an odd modular degree: \( E = 27A, 32A, 36A, 49A, 243B \).

We also verify that all such elliptic curves have rank 0, as predicted by Watkins’s 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.

3.2. **Prime Level.** Let \( E \) be an elliptic curve with an odd congruence number and a prime conductor \( N \). Mestre and Oesterlé \([15]\) have studied 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 Oesterlé also showed that if \( E_{\text{tors}} \) is \( \mathbb{Z}/2\mathbb{Z} \), then \( E \) is a Neumann-Setzer curve and \( N = u^2 + 64 \). Stein and Watkins have studied the parity of congruence number of Neumann-Setzer curves (see \([23]\)) 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 $E_{\text{tors}}$ is nontrivial. Then $L(E, 1) \neq 0$, hence $E(\mathbb{Q})$ has rank 0.

Proof. Recall that

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

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 \cite{14} and \cite{15} (see also \cite{21}) we know that $J_0(N)_{\text{tors}}$ is generated by the cusp $P_1 - P_N$, and for any elliptic curve quotient of $J_0(N) \to E$, $E_{\text{tors}}$ 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 rank of $E(\mathbb{Q})$ is zero by work of \cite{11} and \cite{9}. \hfill \Box

The case when $E$ has a trivial torsion structure and an odd congruence number is studied by Calegari and Emerton (see \cite{3}), where they show that $E$ has an even analytic rank (since $(w_p)_* = -1$), supersingular reductions at 2 and $E(\mathbb{R})$ is connected. Doing a search in the Cremona’s database, it appears that if an elliptic curve $E$ has supersingular reduction at 2, Mordell-Weil rank 0, connected real component, then $E$ will have an odd congruence number.

3.3. Level $N = pq$. In this subsection, we will study 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 \cite{2.14} we know that $p \equiv 3 \pmod{8}$ 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 \cite{2.14} we know that $E[2](\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z})^2$. First, we show that if $E_{\text{tors}}$ 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. Specifically

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 $\overline{Q}$ be the reduction of $Q$ modulo 2. Then $\overline{Q}$ 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

$$E : y^2 + xy = x^3 + a_2x^2 + a_4x.$$ 

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, $4\alpha$, and $\beta$, were $\alpha$ and $\beta$ are both (odd) integers since we are assuming that $E$ is in minimal model. Furthermore, since $E$ is assumed to be semistable, $\alpha$ and $\beta$ are coprime to each other. Note that the point $\left(\frac{\beta}{2}, -\frac{\beta}{2}\right) \in E(\mathbb{Q})$ maps to the identity under the reduction mod 2 map. Using the notation from \cite{21}, we have

$$b_2 = 16\alpha + \beta,$$

$$b_4 = 2\alpha\beta,$$

$$b_6 = 0,$$

$$b_8 = -\alpha^2\beta^2,$$

$$\Delta = \alpha^2\beta^2(16\alpha - \beta)^2.$$
Let \( Q \in E(\mathbb{Q}) \) be a point of order 4, and let \( x(Q) = x_0 \). Recall that we want to show \( 2Q \in E(\mathbb{F}_2) \) is a point of order 4. We have that \( x([2]Q) = 0, 4a, \) or \( \frac{b}{4} \). If \( 2Q \) has order less than 4, then \( 2Q \) must be the identity element, that implies that \( x([2]Q) = \frac{b}{4} \). In that case
\[
\frac{\beta}{4} = \frac{x_0^4 - b_4 x_0^2 - b_4}{4x_0^3 + b_2 x_0^2 + 2b_4 x_0}
\]
\[
= \frac{x_0^4 - 2\alpha \beta x_0^2 + \alpha^2 \beta^2}{4x_0^3 + (16\alpha + \beta)x_0^2 + 4\alpha \beta x_0}
\]
\[
\Rightarrow 0 = x_0^4 - \beta x_0^2 - (6\alpha \beta + \frac{\beta^2}{4})x_0^2 - \alpha^2 \beta^2
\]
\[
= (x_0^2 - \frac{\beta}{2})x_0^2 + \alpha \beta x_0^2 - (4\alpha \beta + \frac{\beta^2}{2})x_0.
\]
Therefore, \( 16\alpha \beta + 2\beta^2 = 2\beta(8\alpha + \beta) \) must be a perfect square; however that is not possible because \( \alpha \) and \( \beta \) are odd. As a result \( x([2]Q) = 0 \) or \( 4a \). Therefore, \( [2]Q \) has order 2 in \( E(\mathbb{F}_2) \). This shows that \( Q \) has order 4, which is the desired result. \( \square \)

**Proposition 3.3.** Let \( E \) be an elliptic curve with conductor \( pq \) and \( E_{\text{tors}} = \mathbb{Z}/2 \times \mathbb{Z}/4 \). Then, \( pq = 15 \) or \( 21 \).

**Proof.** Using the same notation as in lemma 3.2, let \( 0a \) and \( \frac{b}{2} \) be the \( x \)-coordinates of the 2-torsion points of \( E \). Let \( Q \) be a point in \( E_{\text{tors}} \) of order 4. By lemma 3.2, \( x([2]Q) = 0 \) or \( 4a \). Without loss of generality, assume that \( x([2]Q) = 0 \), since if \( x([2]Q) = 4a \), 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 \( \alpha \) and \( \beta \) are coprime, they are both perfect squares, or negative 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. \( \square \)

**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 rules this case out.

**Theorem 3.5.** Assume that \( E \) is an elliptic curve with an odd modular degree. Furthermore, assume that the conductor of \( E \) is \( pq \) with \( pq \neq 21 \) or \( 15 \). Then \( p, q \equiv 3 \pmod{8} \).
Corollary 3.6. Assume that $E$ is an elliptic curve with an odd congruence number and the 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 $\alpha$ and $\beta$, 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 $\pm 16p^r \pm q^s = \pm 1$. We get the same Diophantine equation if $\beta = \pm 1$. Therefore, we need to solve the Diophantine equation

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

Since $q^s \equiv 3 \pmod{8}$ for all odd $s$’s, and $q^s \equiv 1 \pmod{16}$ for all even $s$’s, $s$ must be even and

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

This leads to $(q^{s/2} - 1)(q^{s/2} + 1) = 16p^r$, 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 (mod 8), so we get that $\alpha = \pm 1$.

If $\beta^2 = 1$, then $|16 - \beta|$ 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

$$E : y^2 + x = x^3 + \frac{15 + p^r}{4}x^2 + p^r x.$$
We also have the following

**Theorem 3.7.** Let $E$ be an elliptic curve with conductor $pq$ and an 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 proposition 2.14 we showed that

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

have order two, and $\phi(u)$ and $\phi(u')$ are linearly independent, hence they generate $E[2]$. However, since $p, q = 3 \pmod{8}$ 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 $L(E, 1) \neq 0$. \hfill \Box

### 3.4. Level $N = 2p$.

In this section, we will study 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 $f_E(q) = \sum a_nq^n$ be the modular form attached to the elliptic curve $E$, and let $\Omega_E$ 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 $L_2(f_E, s) = \frac{1}{1 - a_2^{-2s}}$. Similarly

$$\pi(P_p) = 2\pi i \int_{1/2}^{1} f_E(z)dz$$

$$= 2\pi i \int_{0}^{1} f_E(z + 1/2)dz$$

$$= 2\pi i \int_{0}^{i\infty} \sum (-1)^n a_n q^n dz$$

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

$$L(g, s) = (-1 + \frac{a_2}{2^s} + \frac{a_4}{4^s} + \ldots) \prod_{p \geq 2} L_p(f_E, s)$$

$$= \frac{1 - a_2 2^{1-s}}{1 - a_2 2^{-s}} \prod_{p \geq 2} L_p(f_E, s)$$

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 an 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 $\alpha$ is a 2-torsion point in $E$. Since both $\pi(P_p)$ and $\pi(P_{2p})$ are equivalent to real numbers, $\alpha$ is also equivalent to a real number, which implies that $\alpha \equiv \frac{\Omega_E}{2} \pmod{\Omega_E \mathbb{Z}}$. As a result

$$
\pi(P_p) \equiv \pi(P_{2p}) + \frac{\Omega_E}{2} \pmod{\Omega_E \mathbb{Z}},
$$

$$
\Rightarrow -3\pi(P_{2p}) \equiv \frac{\Omega_E}{2} \pmod{\Omega_E \mathbb{Z}},
$$

$$
\Rightarrow \pi(P_{2p}) \equiv \Omega_E\left(\frac{k}{3} - \frac{1}{6}\right) \pmod{\Omega_E \mathbb{Z}}
$$

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 $k \equiv 0 \pmod{3}$), or a 2-torsion point (for $k \equiv 2 \pmod{3}$).

In either case, we have an elliptic curve with a conductor $2p$ and a rational 2-torsion point. Such elliptic curves have been studied by Ivorra [10]. We can use his techniques to put stringent conditions on the values for $p$. Ivorra shows that if $p \geq 29$, then 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 2.3.5 that $p \equiv 7 \pmod{16}$. Putting these two together, we get that $p = 2^k - m^2$. In fact, in this case, Ivorra’s result says that there exists $7 \leq k < f(p)$ where

$$
f(n) = \begin{cases} 
18 + 2 \log_2 n & \text{if } n < 2^{96}, \\
435 + 10 \log_2 n & \text{if } n \geq 2^{96},
\end{cases}
$$

and our elliptic curve is isogeneous to

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

Searching through the Cremona database, we find out that the only elliptic curves with an 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.

3.5. Level $N = 4p$. As with the case of $N = 2p$, we can use Ivorra’s table 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

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

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

We can calculate the rank of such elliptic curves using a standard 2-descent. In fact, if we let $\phi : E \to E'$ and $\phi'$ be the dual isogeny, using the notation from [21] 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

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


gives us $|E(Q)/2E(Q)| \leq 4$. This forces the rank of $E(Q)$ 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.

3.6. Level $N = 8p$. In this case, Ivorra’s table tells us that any elliptic curve with a rational 2-torsion point and the conductor $N = 8p$ satisfies $p \equiv a^2 \pmod{16}$ for $p > 31$. However, by theorem 2.15, $p \equiv 3 \pmod{4}$, 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 an odd congruence number. Furthermore this curve has rank 0.

We will combine all of the above results in

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

1. $E$ has a conductor $p$ and no 2-torsion point, $E$ has supersingular reduction at 2, and $E(R)$ is connected.
2. $E$ has a conductor $p$ and a rational 2-torsion point (hence it is a Neumann-Setzer curve), and $p = u^2 + 64$ with $u \equiv 3 \pmod{8}$.
3. $E$ has a 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 a conductor $4p$ and $p = m^2 + 4$ for some integer $m \equiv 1 \pmod{4}$, and $E$ is isogenous to one of
   \[y^2 = x^3 + mx^2 - x.\]
5. $E$ has a conductor $pq$ with $p$ and $q$ being odd primes, $p \equiv q \equiv 3 \pmod{8}$, and for some odd integers $r$ and $s$, $p^r - q^s = 16$, 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, 43A, 243B.

In all of the above cases, $E$ has rank 0, except possibly in case 4. In this case, we know that $E$ has an even analytic rank.

Note that all of the curves in case 6 in the above theorem have a non-trivial torsion point. Therefore we have proved that if $E$ has odd congruence number and has a nontrivial torsion point, then it has rank 0. Also note that for all of the above cases, except for case 1, we construct a family of elliptic curves with all the desired torsion structures and conductors. We expect that all of these elliptic curves have odd congruence numbers. This can be proved if, for example, we show that $J_0(N)[m] \rightarrow E[2]$ is injective and $J[m] = C_N[m]$. When $E$ is a Neumann-Setzer curve, the results of [14] and [15] prove this result. We expect that similar results are true for the other cases; however we, do not yet know of a proof of this result.

Finally, it is natural to ask how often do elliptic curves have odd congruence number. Since such elliptic curves can not have more than three primes dividing their conductor, they are not that common. Furthermore as soon as we have a nontrivial rational torsion point, we have a conjectural parametrization of all such
elliptic curves. Therefore we like to know how often we get an optimal elliptic curve of prime conductor with no rational torsion point having an odd modular degree. Looking through Cremona’s table of elliptic curves of conductor less than 130000, we find 1991 elliptic curves of prime conductor and trivial rational torsion structure, out of which 196 of those have an odd modular degree.

References

[1] A. Agashe, K. A. Ribet, and W. A. Stein. The modular degree, congruence primes, and multiplicity one. preprint.
[2] 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):843–939 (electronic), 2001.
[3] F. Calegari and M. Emerton. Elliptic curves of odd modular degree. Israel Journal of Mathematics, 169:417–444, 2009.
[4] 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):2255–2263, 1997.
[5] J. Cremona and M. Watkins. data available at http://www.warwick.ac.uk/staff/J.E.Cremon/ftp/data/INDEX.html.
[6] N. Dummigan. On a conjecture of Watkins. J. Théor. Nombres Bordeaux, 18(2):345–355, 2006.
[7] M. Emerton. Optimal quotients of modular Jacobians. Math. Ann., 327(3):429–458, 2003.
[8] G. Frey. On ternary equations of Fermat type and relations with elliptic curves. In Modular forms and Fermat’s last theorem (Boston, MA, 1995), pages 527–548. Springer, New York, 1997.
[9] B. H. Gross and D. B. Zagier. Heegner points and derivatives of $l$-series. Invent. Math., 84(2):225–320, 1986.
[10] W. Ivorra. Courbes elliptiques sur $\mathbb{Q}$ ayant un point d’ordre 2 rationnel sur $\mathbb{Q}$, de conducteur $2^np$. Dissertationes Math. (Rozprawy Mat.), 429:55, 2004.
[11] V. A. Kolyvagin. Finiteness of $\mathfrak{e}(\mathbb{Q})$ and $\mathfrak{s}b(c, q)$ for a subclass of weil curves. Izv. Akad. Nauk SSSR Ser. Mat., 52(3):522–540, 670–671, 1988.
[12] G. Ligozat. Courbes modulaires de genre 1. Société Mathématique de France, Paris, 1975.
[13] S. Ling. On the $\mathbb{Q}$-rational cuspidal subgroup and the component group of $J_0(p^r)$. Israel J. Math., 99:29–54, 1997.
[14] B. Mazur. Modular curves and the Eisenstein ideal. Inst. Hautes Études Sci. Publ. Math., (47):33–186 (1978), 1977.
[15] J.-F. Mestre and J. Oesterlé. Courbes de Weil semi-stables de discriminant une puissance m-ième. J. Reine Angew. Math., 400:173–184, 1989.
[16] M. R. Murty. Bounds for congruence primes. In Automorphic forms, automorphic representations, and arithmetic (Fort Worth, TX, 1996), volume 66 of Proc. Sympos. Pure Math., pages 177–192. Amer. Math. Soc., Providence, RI, 1999.
[17] A. P. Ogg. Hyperelliptic modular curves. Bull. Soc. Math. France, 102:449–462, 1974.
[18] K. A. Ribet. Twists of modular forms and endomorphisms of abelian varieties. Math. Ann., 253(1):43–62, 1980.
[19] K. A. Ribet. Endomorphism algebras of abelian varieties attached to newforms of weight 2. In Seminar on Number Theory, Paris 1979–80, volume 12 of Progr. Math., pages 263–276. Birkhäuser Boston, Mass., 1981.
[20] G. Shimura. Introduction to the arithmetic theory of automorphic functions, volume 11 of Publications of the Mathematical Society of Japan. Princeton University Press, Princeton, NJ, 1994.
[21] J. H. Silverman. The arithmetic of elliptic curves, volume 106 of Graduate Texts in Mathematics. Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original.
[22] W. A. Stein and M. Watkins. A database of elliptic curves—first report. In Algorithmic number theory (Sydney, 2002), volume 2369 of Lecture Notes in Comput. Sci., pages 267–275. Springer, Berlin, 2002.
[23] W. A. Stein and M. Watkins. Modular parametrizations of Neumann-Setzer elliptic curves. Int. Math. Res. Not., (27):1395–1405, 2004.
[24] M Watkins. Computing the modular degree of an elliptic curve. *Experimental Mathematics*, 11(3):487–502, 2000.

McMaster University

_E-mail address:_ syazdani@math.mcmaster.ca