VERBOSE VERSION

RATIONAL POINTS ON $X_0^+(N)$ AND QUADRATIC $\mathbb{Q}$-CURVES

STEVEN D. GALBRAITH

ABSTRACT. We consider the rational points on $X_0(N)/W_N$ in the case where N is a composite number. We give an experimental study of some of the cases not covered by the results of Momose. We find exceptional rational points in the cases $N = 91$ and $N = 125$. and we exhibit the j-invariants of the corresponding quadratic $\mathbb{Q}$-curves.

1. Introduction

Let N be an integer greater than one. Let $X_0(N)$ be the modular curve whose non-cusp points correspond to isomorphism classes of isogenies between elliptic curves $\phi : E \to E'$ of degree N with cyclic kernel. The Fricke involution W_N on $X_0(N)$ arises from taking the dual isogeny (see [31]) $\widehat{\phi} : E' \to E$. We define the modular curve $X_0^+(N)$ to be the quotient of $X_0(N)$ by the group of two elements generated by W_N. It is known that $X_0(N)$ has a model over $\mathbb{Q}$ and that the action of W_N is also defined over $\mathbb{Q}$. Therefore there is a model for $X_0^+(N)$ over $\mathbb{Q}$ and one can study the $\mathbb{Q}$-rational points on this curve.

The results of Mazur [24], Kenku [21] and others have completely classified the rational points on the modular curves $X_0(N)$. In particular, it was shown that for $N > 37$ the only rational points on $X_0(N)$ are cusps and points corresponding to certain elliptic curves with complex multiplication (and of course the number of CM cases is finite). In the famous case $X_0(37)$ the modular curve is hyperelliptic but the involution is not an Atkin-Lehner involution. The images of the rational cusps of $X_0(37)$ under the hyperelliptic involution are 'exceptional' rational points.

The modular curves $X_0^+(N)$ are also an interesting object of study (for instance, due to their connection with $\mathbb{Q}$-curves). Momose [25], [26] has given some results of a similar nature to those of Mazur but the results only apply to certain composite values of N. Therefore, a classification of rational points on $X_0^+(N)$ is not yet complete.

In this paper we use computational methods to determine some exceptional rational points on $X_0^+(N)$ in cases where N is composite and not covered by the results of Momose. This continues the work of [10] which gave a computational study of the case when N is a prime number.

The most interesting examples given in this paper are the modular curves $X_0^+(91)$ and $X_0^+(125)$. As with $X_0(37)$, these are hyperelliptic curves but the hyperelliptic involution is not an Atkin-Lehner involution. We find exceptional rational points in these cases.

The conclusion is the following: We conjecture that the only N for which the genus of $X_0^+(N)$ is between 2 and 5 and such that $X_0^+(N)$ has exceptional rational

Date: February 1, 2011.

points are 73, 91, 103, 125, 137, 191 and 311. One further contribution of the paper is the conjecture that $X_{split}(p)$ (which is isomorphic to $X_0^+(p^2)$) has no exceptional rational points when $p = 13$. This result has implications in the study of two dimensional Galois representations.

The first sections of the paper recall some well-known results on modular curves and their points. Sections 6 to 8 are concerned with some properties of Heegner points on $X_0^+(N)$. Section 9 recalls the results of Momose. The remaining sections deal with the experimental results.

2. Rational points on $X_0^+(N)$

The non-cusp points of $X_0^+(N)$ can be interpreted as pairs $\{\phi : E \to E', \widehat{\phi} : E' \to E\}$. From [6] it is known that if a non-cusp point of $X_0^+(N)$ is defined over a field L then the corresponding pair of isogenies and elliptic curves may also be taken to be defined over L. Therefore the only possibilities for rational points on $X_0^+(N)$ are as follows.

Proposition 1. *A non-cusp rational point on $X_0^+(N)$ corresponds to a pair $\{\phi : E \to E', \widehat{\phi} : E' \to E\}$ such that one of the following holds.*

1. *E, E', ϕ and $\widehat{\phi}$ are all defined over $\mathbb{Q}$.*
2. *E and E' are defined over $\mathbb{Q}$, the isogeny ϕ is defined over a quadratic field L, and the non-trivial element $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ is such that $\phi^\sigma \cong \widehat{\phi}$ and so $E \cong E'$.*
3. *E, E', ϕ and ϕ' are defined over a quadratic field L, $E \not\cong E'$, and the non-trivial element $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ is such that $\phi^\sigma \cong \widehat{\phi}$ and $E' \cong E^\sigma$.*

The first case is the case of rational points on $X_0(N)$, and these have been classified. The second and third cases will be discussed further in Sections 5 and 6.

3. Cusps of $X_0^+(N)$

Over $\mathbb{C}$ we have that $X_0(N)$ is isomorphic to the quotient $\Gamma_0(N)\backslash\mathcal{H}^*$ where $\mathcal{H}^* = \{z \in \mathbb{C} : Im(z) > 0\} \cup \mathbb{P}^1(\mathbb{Q})$, and the group $\Gamma_0(N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod N\}$ acts (on the left) on $\mathcal{H}^*$ by linear fractional transformations. The cusps correspond to the $\Gamma_0(N)$-orbits of $\mathbb{P}^1(\mathbb{Q})$.

There are cusps on $X_0(N)$ for every divisor $d|N$. The cusps correspond to elements $[x : d] \in \mathbb{P}^1(\mathbb{Q})$ where x runs over the elements of $(\mathbb{Z}/\gcd(d, N/d)\mathbb{Z})^*$ (see Ogg [28]). There are $t_d = \varphi(\gcd(d, N/d))$ such cusps and they are defined over some number field $L \subset \mathbb{Q}(\zeta_d)$ of degree t_d over $\mathbb{Q}$. In particular, the cusps are rational if and only if $t_d = 1$. The involution W_N maps $[x : d]$ to $[-x^{-1} : N/d]$.

Pairs $\{[x : d], [-x^{-1} : N/d]\}$ of rational cusps on $X_0(N)$ give rise to rational cusps on $X_0^+(N)$. The following result is easily proved.

Proposition 2. *The only integers N for which non-rational cusps of $X_0(N)$ can give a rational cusp on $X_0^+(N)$ are $N \in \{9, 16, 36\}$. The corresponding cusps are $\{[1 : \sqrt{N}], [-1 : \sqrt{N}]\}$.*

4. Atkin-Lehner involutions

For every divisor $n|N$ such that $\gcd(n, N/n) = 1$ the Atkin-Lehner involution [1] on $X_0(N)$ is defined by $W_n(E, C) = (E/C[n], (E[n] + C)/C[n])$ where E is the

elliptic curve, C is the cyclic kernel of the N-isogeny, and $E[n]$ and $C[n]$ denote the elements of order n of the corresponding group.

Over $\mathbb{C}$ we can define the Atkin-Lehner involutions as elements of $\Gamma_0(N)\backslash \mathrm{SL}_2(\mathbb{R})$ as follows. Let $a, b, c, d \in \mathbb{Z}$ be such that $adn - bcN/n = 1$ and define $W_n = \frac{1}{\sqrt{n}}\left(\begin{smallmatrix} na & b \\ Nc & nd \end{smallmatrix}\right)$. This construction is well-defined up to multiplication by $\Gamma_0(N)$ and therefore each W_n gives an involution on the modular curve $X_0(N)$. Note that if $\gcd(n_1, n_2) = 1$ then $W_{n_1 n_2} = W_{n_1} W_{n_2}$.

The W_n also give rise to involutions on $X_0^+(N)$. If $n \notin \{1, N\}$ then W_n is non-trivial and the action of W_n and $W_{N/n}$ is identical. The Atkin-Lehner involutions are defined over $\mathbb{Q}$ and so they map L-rational points of $X_0(N)$ to L-rational points for any field $L/\mathbb{Q}$. Furthermore the Atkin-Lehner involutions map cusps to cusps.

5. Quadratic $\mathbb{Q}$-curves

In Section 6 we discuss points corresponding to elliptic curves with complex multiplication (CM). For the remainder of this section we consider the case of points which do not arise in this way. A rational point of $X_0^+(N)$ which is neither a cusp, nor corresponds to a rational point of $X_0(N)$ or an elliptic curve with complex multiplication will be called 'exceptional'.

We state a result of Elkies concerning the interpretation of these exceptional rational points as $\mathbb{Q}$-curves. Recall that a $\mathbb{Q}$-curve is an elliptic curve E over a number field L which is isogenous to all its Galois conjugates [15], [30]. By a 'quadratic $\mathbb{Q}$-curve' we mean a $\mathbb{Q}$-curve E which is defined over some quadratic number field $L/\mathbb{Q}$ and which cannot be defined over $\mathbb{Q}$.

Theorem 1. *(Elkies [7]) Every quadratic $\mathbb{Q}$-curve without complex multiplication (CM) corresponds to a rational point on $X_0^+(N)$ for some $N > 1$. Conversely, every non-cusp rational point on $X_0^+(N)$ corresponds either to an elliptic curve with CM, to a rational point of $X_0(N)$, or to a non-CM quadratic $\mathbb{Q}$-curve.*

Proof. Let E be a $\mathbb{Q}$-curve over a quadratic field L. Write σ for the non-trivial element of $\mathrm{Gal}(L/\mathbb{Q})$. Then, by hypothesis, there is some isogeny $\phi : E \to E^\sigma$. Define N to be the degree of ϕ. Since E does not have CM it follows that $\phi^\sigma \circ \phi = [\pm N] \in \mathrm{End}(E)$. In the case of $[-N]$ above we can compose ϕ^σ with the automorphism $[-1]$ since points of the modular curve correspond only to isomorphism classes of isogenies. It follows that $\phi^\sigma \cong \widehat{\phi}$ and that we have a rational point on $X_0^+(N)$.

The converse follows from Proposition 1. The second case of that Proposition is necessarily a CM curve. In the third case the elliptic curve may have CM, but if not then we have a non-CM quadratic $\mathbb{Q}$-curve. □

Elkies proves further that every quadratic $\mathbb{Q}$-curve is isogenous to a quadratic $\mathbb{Q}$-curve curve which corresponds to a rational point on some $X_0^+(N)$ where N is square-free.

6. Heegner points

A Heegner point of $X_0(N)$ is a non-cusp point corresponding to an isogeny of elliptic curves $\phi : E \to E'$ such that both E and E' have complex multiplication by the same order $\mathcal{O}$ of discriminant D in the quadratic field $K = \mathbb{Q}(\sqrt{D})$. In this case we say that the Heegner point has discriminant D.

For the remainder of this paper we will use the following standard notation. We write $\langle \alpha, \beta \rangle$ for the lattice generated by α and β over $\mathbb{Z}$. An elliptic curve E over $\mathbb{C}$ is isomorphic to a complex torus $\mathbb{C}/\langle 1, \tau \rangle$ where $\tau \in \mathbb{C}$ has positive imaginary part. Two such elliptic curves are isomorphic if and only if the corresponding values of τ are related by some $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ (acting as a linear fractional transformation). The endomorphism ring $\mathrm{End}(E)$ is isomorphic to the $\mathbb{Z}$-module $\{\lambda \in \mathbb{C} : \lambda, \lambda\tau \in \langle 1, \tau \rangle\}$. One has $\mathrm{End}(E) \neq \mathbb{Z}$ if and only if τ is imaginary quadratic, in which case $\mathrm{End}(E)$ is an order $\mathcal{O}$ in the quadratic field $\mathbb{Q}(\tau)$. Orders in imaginary quadratic fields are uniquely determined by their discriminant D via $\mathcal{O} \cong \mathbb{Z}[(D + \sqrt{D})/2]$. The conductor of an order $\mathcal{O}$ of discriminant D is the largest positive integer c such that $D/c^2 \equiv 0, 1 \pmod 4$. The lattice $\langle 1, \tau \rangle$ is a projective $\mathcal{O}$-module (or 'proper $\mathcal{O}$-lattice' in the language of Lang [23]). The group of classes of projective $\mathcal{O}$-modules is denoted $\mathrm{Pic}(\mathcal{O})$. The order of the group $\mathrm{Pic}(\mathcal{O})$ is called the class number of $\mathcal{O}$.

The importance of Heegner points in the present context is due to the following.

Proposition 3. *Suppose that the genus of $X_0^+(N)$ is at least one. Then a non-cusp rational point on $X_0^+(N)$ corresponding to an elliptic curve with complex multiplication (CM) is necessarily a Heegner point.*

Proof. Proposition 1 gives three possibilities for a non-cusp rational point of $X_0^+(N)$. Suppose now that one of the corresponding elliptic curves has CM, then the isogenous elliptic curve must also have CM by an order in the same quadratic field.

The first case can only occur when the class number is one and either $E \cong E'$ (and we have a Heegner point) or $E \ncong E'$ and the isogeny is between two elliptic curves whose endomorphism rings are different orders in the same quadratic field. The only cases when this arises is when one of the curves has CM of discriminant $D = -12, -16, -27$ or -28. The isogeny itself must be composed of an isogeny of degree equal to the conductor of the order (see Proposition 11), followed by rational isogeny (i.e., one corresponding to a ramified ideal, see Theorem 3). Therefore the only candidate degrees for cyclic rational isogenies are $N = 2, 3, 4, 6, 9, 14$ and the genus of $X_0^+(N)$ is zero in all these cases.

Finally, in the second and third cases we have $\mathrm{End}(E) \cong \mathrm{End}(E')$ and so the point is a Heegner point. □

The following result is well known (see [3], [16], [10]).

Theorem 2. *Heegner points on $X_0(N)(\mathbb{C})$ are in one-to-one correspondence with $\Gamma_0(N)$-equivalence classes of quadratic forms $NAX^2+BXY+CY^2$ where $A, B, C \in \mathbb{Z}$ are such that $A, C > 0$ and $\gcd(NA, B, C) = \gcd(A, B, NC) = 1$.*

Note that the $\Gamma_0(N)$-equivalence class of a quadratic form $NAX^2+BXY+CY^2$ is simply the set of all forms $NA(aX+bY)^2+B(aX+bY)(cX+dY)+C(cX+dY)^2$ where $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$.

The correspondence mentioned in Theorem 2 is as follows. Let τ be the root of $NA\tau^2 + B\tau + C = 0$ with positive imaginary part. Then $E = \mathbb{C}/\langle 1, \tau \rangle$ is an elliptic curve with complex multiplication by the order $\mathcal{O}$ of discriminant $D = B^2 - 4NAC$ and the cyclic isogeny with kernel $\langle \frac{1}{N}, \tau \rangle$ maps to the elliptic curve $E' \cong \mathbb{C}/\langle 1, \frac{-1}{N\tau} \rangle$ which also has CM by $\mathcal{O}$ (see Lang [23] Theorem 8.1).

In particular, a Heegner point on $X_0(N)$ of discriminant D can only arise when the primes $p|N$ satisfy $(\frac{D}{p}) \neq -1$. However this condition is not sufficient since

there can be cases where all $p|N$ split or ramify and yet one cannot find a suitable triple (A, B, C) as above.

The Atkin-Lehner involutions W_n (where $n|N$ is such that $\gcd(n, N/n) = 1$) map Heegner points to Heegner points with the same discriminant. Therefore it makes sense to speak of Heegner points on $X_0^+(N)$.

Proposition 4. *Suppose the genus of $X_0^+(N)$ is at least one. Let $n|N$ be such that $\gcd(n, N/n) = 1$ and $n \notin \{1, N\}$. A rational point of $X_0^+(N)$ which is fixed by the Atkin-Lehner involution W_n must be a cusp or a Heegner point.*

Proof. (Also see Gross [17] Proposition 3.1) Such a rational point corresponds to some $\tau \in \mathcal{H}^*$ such that $W_n(\tau) = \gamma(\tau)$ for some $\gamma \in \Gamma_0(N)$. It follows that τ satisfies a quadratic equation over $\mathbb{Z}$ and so we either have a cusp or a CM point. The result follows from Proposition 3. □

An immediate corollary to this result is the following.

Proposition 5. *Suppose the genus of $X_0^+(N)$ is at least one. Let $\omega(N)$ be the number of distinct primes dividing N. Then the exceptional rational points of $X_0^+(N)$ (if there are any) fall into orbits under the Atkin-Lehner involutions of the full size $2^{\omega(N)-1}$.*

7. Rationality of Heegner Points on $X_0^+(N)$

In the context of this paper it is important to determine when Heegner points of $X_0(N)$ can give a rational point of $X_0^+(N)$. The relevant results have already been deduced by Gross [16] using the theory of complex multiplication and we recall them here.

Let $\phi : E \to E'$ be a Heegner point on $X_0(N)$ with $\mathrm{End}(E) = \mathcal{O}$ an order of discriminant D in a quadratic imaginary field K. Then, as in Theorem 2, over $\mathbb{C}$, there is some τ such that $NA\tau^2 + B\tau + C = 0$, $D = B^2 - 4NAC$, $E \cong \mathbb{C}/\langle 1, \tau\rangle$ and $E' \cong \mathbb{C}/\langle 1/N, \tau\rangle$.

Following Gross [16] we write $\mathfrak{a}$ for the projective $\mathcal{O}$-module $\langle 1, \tau\rangle$ (the isomorphism class of the elliptic curve E depends only on the class of $\mathfrak{a}$ in $\mathrm{Pic}(\mathcal{O})$) and write $\mathfrak{b}$ for $\langle 1/N, \tau\rangle$. The isogeny ϕ then corresponds to the projective $\mathcal{O}$-module $\mathfrak{n} = \mathfrak{a}\mathfrak{b}^{-1}$ which in this case is the $\mathcal{O}$-module $\langle N, (-B + \sqrt{D})/2\rangle$.

We emphasise that the elliptic curve E only depends on the *class* of the module $\mathfrak{a}$ whilst the isogeny depends on the *specific* module $\mathfrak{n}$ rather than its class. The fact that the kernel is cyclic may be expressed as $\mathcal{O}/\mathfrak{n} \cong \mathbb{Z}/N\mathbb{Z}$. Gross uses the notation $(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])$ for the Heegner point.

Theorem 3. *(Gross [16]) The Heegner point $(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])$ on $X_0(N)$ is defined over the ring class field $H_\mathcal{O}$. Furthermore:*

1. *Complex conjugation acts on $(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])$ as $\overline{(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])} = (\mathcal{O}, \overline{\mathfrak{n}}, [\mathfrak{a}]^{-1})$.*
2. *The group $\mathrm{Gal}(H_\mathcal{O}/K)$ acts on $(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])$ as follows: For $\sigma \in \mathrm{Gal}(H_\mathcal{O}/K)$ let $\mathfrak{b} \in \mathrm{Pic}(\mathcal{O})$ be a projective $\mathcal{O}$-module (prime to the conductor of $\mathcal{O}$) corresponding to σ via the Artin map. Then $(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])^\sigma = (\mathcal{O}, \mathfrak{n}, [\mathfrak{a}\mathfrak{b}^{-1}])$.*
3. *The Atkin-Lehner involution W_N maps $(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])$ to $(\mathcal{O}, \overline{\mathfrak{n}}, [\mathfrak{a}\mathfrak{n}^{-1}])$.*

Proof. Note that Gross states this result only when $\gcd(N, c) = 1$. The theory of complex multiplication shows that the elliptic curves E and E' are defined over the ring class field $H_\mathcal{O}$. Thus the Heegner point is defined over some finite abelian

extension of $H_{\mathcal{O}}$. Recall that $Gal(H_{\mathcal{O}}/\mathbb{Q})$ is isomorphic to the semidirect product of $\mathrm{Pic}(\mathcal{O})$ with the group $Gal(K/\mathbb{Q})$ of order two generated by complex conjugation.

Property 1 is clear (see Lang [23] Remark 10.2 page 134). Property 2 follows from Lang [23] Theorem 10.5. Property 3 follows from the fact that W_N maps (E, C) to $(E/C, E[N]/C)$.

Finally, suppose that the Heegner point is defined over some (Galois) extension L. Then $L/H_{\mathcal{O}}$ is abelian and the theory of complex multiplication shows that the action of any element of $Gal(L/H_{\mathcal{O}})$ corresponds to some ideal $\mathfrak{b}$. This action therefore maps the Heegner point $\mathbb{C}/\mathfrak{a} \rightarrow \mathbb{C}/\mathfrak{a}\mathfrak{n}^{-1}$ to $\mathbb{C}/\mathfrak{a}\mathfrak{b}^{-1} \rightarrow \mathbb{C}/\mathfrak{a}\mathfrak{b}^{-1}\mathfrak{n}^{-1}$ which is isomorphic to the original point. Thus the Heegner point is defined over $H_{\mathcal{O}}$. □

From this we easily deduce the following.

Theorem 4. *Let $x = \{\phi : E \rightarrow E', \widehat{\phi} : E' \rightarrow E\}$ be a Heegner point of $X_0^+(N)$ with $\mathrm{End}(E) = \mathcal{O}$. Let $\mathfrak{n}$ be the projective $\mathcal{O}$-module corresponding to the isogeny. Then x is defined over $\mathbb{Q}$ if and only if either*

1. *$h_{\mathcal{O}} = 1$, or*
2. *$h_{\mathcal{O}} = 2$, $\mathfrak{n}$ is not principal and $\mathfrak{n} = \overline{\mathfrak{n}}$.*

Proof. By Theorem 3, a Heegner point of $X_0^+(N)$ is defined over $H_{\mathcal{O}}$. The Galois group $\mathrm{Gal}(H_{\mathcal{O}}/\mathbb{Q})$ is the semidirect product of $\mathrm{Gal}(H_{\mathcal{O}}/K)$ with $\mathrm{Gal}(K/\mathbb{Q})$. Therefore, we obtain a rational point of $X_0^+(N)$ if and only if the set $\{(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}]), (\mathcal{O}, \overline{\mathfrak{n}}, [\mathfrak{a}\mathfrak{n}^{-1}])\}$ is fixed by these two Galois groups.

The action of $\mathrm{Gal}(H_{\mathcal{O}}/K)$ is trivial in the class number one case and it maps $\mathbb{C}/\mathfrak{a}$ to $\mathbb{C}/\mathfrak{a}\mathfrak{b}^{-1}$ where $\mathfrak{b}$ is non-principal in the class number two case. It follows that, in the class number two case, the Heegner point is invariant under $Gal(H_{\mathcal{O}}/K)$ if and only if $\mathfrak{n}$ is non-principal.

The action of $\mathrm{Gal}(K/\mathbb{Q})$ does not change the isomorphism class of $\mathbb{C}/\mathfrak{a}$ but it may change the isogeny. Hence, in the class number two case one must have $\mathfrak{n} = \overline{\mathfrak{n}}$. □

We now discuss the meaning of the condition $\mathfrak{n} = \overline{\mathfrak{n}}$. In terms of the representation $\mathfrak{n} = \langle N, (B + \sqrt{D})/2 \rangle$ we see that $\mathfrak{n} = \overline{\mathfrak{n}}$ if and only if $N | B$. In the case when N is coprime to the conductor of $\mathcal{O}$ it follows that every prime p dividing N must ramify in $\mathcal{O}$, and therefore N must be square-free. The case when N is not coprime to the conductor of $\mathcal{O}$ will be discussed in more detail in Section 8.

We could end the analysis here, since Theorem 2 tells when a Heegner point of $X_0(N)$ can arise (and can be used as the basis of an algorithm to list all $\Gamma_0(N)$-equivalence classes of suitable τ) while Theorem 4 tells when they give rational points of $X_0^+(N)$. Thus, from a computational point of view, we have all the tools we need. However, there are some hidden subtleties regarding orders whose conductors are not coprime to N and it would be dishonest not to give further explanation.

8. The Action of Atkin-Lehner Involutions on Heegner Points

Let $n | N$ be such that $\gcd(n, N/n) = 1$ and consider the Atkin-Lehner involution W_n. One can show that W_n maps the isogeny $\phi : \mathbb{C}/\langle 1, \tau \rangle \rightarrow \mathbb{C}/\langle 1/N, \tau \rangle$ to the isogeny $\phi' : \mathbb{C}/\langle 1, n\tau \rangle \rightarrow \mathbb{C}/\langle n/N, \tau \rangle$.

We first consider the case where $\gcd(N, c) = 1$.

Proposition 6. *(Gross [16]) Let $(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])$ be a Heegner point on $X_0(N)$ with N coprime to the conductor of $\mathcal{O}$. Suppose $p^\alpha \| N$ and suppose $\mathfrak{n} = \mathfrak{p}^\alpha \mathfrak{m}$ where p decomposes as $\mathfrak{p}\overline{\mathfrak{p}}$ in $\mathcal{O}$. Then the Atkin-Lehner involution W_{p^α} acts by $W_{p^\alpha}(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}]) = (\mathcal{O}, \overline{\mathfrak{p}}^\alpha \mathfrak{m}, [\mathfrak{a}\mathfrak{p}^{-\alpha}])$.*

The following result is then immediate.

Proposition 7. *Let N be a positive integer. Let $\mathcal{O}$ be an order of conductor coprime to N for which there exist rational Heegner points on $X_0^+(N)$. Let $\omega'(N)$ be the number of distinct primes dividing N which split in $\mathcal{O}$.*

1. *If the class number of $\mathcal{O}$ is one then there are $\max\{1, 2^{\omega'(N)-1}\}$ rational Heegner points on $X_0^+(N)$ corresponding to the order $\mathcal{O}$ and they are all mapped to each other by Atkin-Lehner involutions.*
2. *If the class number of $\mathcal{O}$ is two then there is only one such Heegner point (i.e., $\omega'(N) = 0$ and it is fixed by all the Atkin-Lehner involutions).*

Proof. From the above arguments and the notation $(\mathcal{O}, \mathfrak{n}, [\mathfrak{a}])$ it follows that the set of all rational Heegner points on $X_0^+(N)$ corresponding to an order $\mathcal{O}$ is obtained by taking the images of one of them under the group of Atkin-Lehner involutions.

The statements about the number of rational points which arise then follow from Proposition 6. □

We emphasise that the property of all Heegner points being related by Atkin-Lehner involutions is special to the case of *rational* points on $X_0^+(N)$. For instance, if $\mathcal{O}$ has class number three or more then obviously all Heegner points on $X_0^+(p)$ (where p is prime) cannot be related by Atkin-Lehner involutions.

As seen in [10], rational Heegner points coming from class number two orders are rather rare.

Proposition 8. *Let D be the discriminant of an order of class number two and conductor c. Then for $N > 89$ coprime to c, there are no rational Heegner points on $X_0^+(N)$ corresponding to the discriminant D.*

Proof. In this case we require that N be square-free and that all primes $p|N$ ramify (i.e., $N|D$).

The list of all class number two discriminants D is -15, $-20, -24, -32, -35$, $-36, -40, -48, -51$, $-52, -60, -64, -72$, $-75, -88, -91$, -99, $-100, -112$, -115, -123, $-147, -148, -187$, $-232, -235, -267$, -403, -427. This already severely limits the number of possible values of square-free N for which $N|D$.

A further condition is that the projective $\mathcal{O}$-module $\mathfrak{n}$ which has norm N must satisfy $\mathfrak{n} = \overline{\mathfrak{n}}$ and be non-principal. For most of the larger discriminants in the list one sees that D is itself square-free and that by unique factorisation the only ideal of norm $N = -D$ is the ideal $(\sqrt{D})$ which is principal.

One can check that 89 is the largest N for which $N|D$, $\gcd(N, c) = 1$ and for which a suitable ideal $\mathfrak{n}$ exists. Indeed, there is a rational point on the genus one curve $X_0^+(89)$ corresponding to the class number two discriminant $D = -267$. □

There are further examples of rational Heegner points of class number two. For instance, in Section 11 it is shown that the curve $X_0^+(74)$ is an example of a composite value of N for which there is a rational a class number two heegner point.

We now consider the case where N is not coprime to the conductor of $\mathcal{O}$.

The following result is well-known. An explicit proof for elliptic curves over $\mathbb{C}$ may be found in the appendix to [11].

Proposition 9. *Let E be an elliptic curve over $\mathbb{C}$ such that $\mathrm{End}(E) \cong \mathcal{O}$ of discriminant D. Suppose p is a prime dividing the conductor of $\mathcal{O}$. Then, up to isomorphism, there is exactly one p-isogeny from E 'up' to an elliptic curve E' such that $\mathrm{End}(E')$ has discriminant D/p^2 and that there are exactly p isogenies of degree p from E 'down' to elliptic curves whose endomorphism ring has discriminant p^2D. If p does not divide the conductor of $\mathcal{O}$ then there are $1+(\frac{D}{p})$ isogenies of degree p to elliptic curves E' with $\mathrm{End}(E') = \mathcal{O}$ and there are $p-(\frac{D}{p})$ isogenies of degree p down to elliptic curves whose endomorphism ring has discriminant p^2D.*

Returning to the context of Heegner points, we have the following. Note that I write $f \circ g$ for the composition of functions $f(g(\cdot))$.

Proposition 10. *Suppose $\phi : E \rightarrow E'$ is a Heegner point on $X_0(N)$ of discriminant D and that p is a prime dividing $\gcd(N, c)$. Then ϕ factors as $\psi_2 \circ \psi \circ \psi_1$ where*

1. *ψ_1 is an isogeny of degree p up from E to an elliptic curve E_1 whose endomorphism ring has discriminant D/p^2.*
2. *ψ is an isogeny of degree N/p^2 from E_1 to some elliptic curve E_2 such that $\mathrm{End}(E_2)$ has discriminant D/p^2.*
3. *ψ_2 is an isogeny of degree p from E_2 down to E'.*

Proof. We can write E as $\mathbb{C}/\langle 1, \tau\rangle$ where τ satisfies $NA\tau^2 + B\tau + C = 0$. From the condition $p|D = B^2 - 4NAC$ we have $p|B$. One can show that $p^2|N$. The isogeny ϕ has kernel $\langle 1/N, \tau\rangle$ and we define ψ_1 to be the isogeny having kernel $\langle 1/p, \tau\rangle$. This isogeny maps E to $E_1 = \mathbb{C}/\langle 1/p, \tau\rangle \cong \mathbb{C}/\langle 1, p\tau\rangle$ where $p\tau$ satisfies $(NA/p^2)X^2 + (B/p)X + C = 0$ and so the elliptic curve E' has complex multiplication by the order of discriminant D/p^2.

The remaining statements are now immediate. □

Indeed, when $\gcd(p, N/p^2) = 1$ then we can also factor ϕ as $\psi' \circ \psi_2 \circ \psi_1$ or $\psi_2 \circ \psi_1 \circ \psi'$ (where ψ' here is an N/p^2-isogeny between elliptic curves whose endomorphism rings have discriminant D).

I call the following the 'no-down-up' result.

Proposition 11. *Let ϕ be an N-isogeny with cyclic kernel. Then ϕ cannot be factored as $\psi_1 \circ \psi_2 \circ \cdots \circ \psi_n$ where ψ_i is some isogeny of prime degree p up and ψ_j for $j > i$ is some p-isogeny down.*

Proof. If such a factorisation exists then it is possible to obtain a factorisation for which there are two consecutive p-isogenies ψ_i and ψ_{i+1} such that ψ_i goes up and ψ_{i+1} goes down. Since isogenies up are unique we must have $\psi_i \cong \widehat{\psi}_{i+1}$ and thus the composition does not have cyclic kernel. □

The following result is now clear.

Theorem 5. *Suppose N is a positive integer and that $\mathcal{O}$ is an order of discriminant D and conductor c in an imaginary quadratic field K. Let d be the largest positive integer such that $d|c$ and $d^2|N$. Then there can be a Heegner point on $X_0(N)$ corresponding to the order $\mathcal{O}$ only if $\gcd(N/d^2, c/d) = 1$.*

In general, the isogenies down from an elliptic curve map to different elliptic curves. However, there are some exceptions to this rule in the cases when $\mathrm{End}(E)$ has units other than ± 1. In particular, this can arise when $\mathrm{End}(E)$ has discriminant -3 or -4. We see that there are isogenies $\psi, \psi' : E \to E'$ down which are isomorphic in the sense that $\psi' = \psi \circ \varepsilon$ where ε is a unit in $\mathrm{End}(E)$. Note that both ψ and ψ' have the same dual isogeny (which is the unique isogeny up from E' to E) and that the isogenies $\widehat{\psi} \circ \psi$ and $\widehat{\psi} \circ \psi'$ are isomorphic while the isogenies $\psi \circ \widehat{\psi}$ and $\psi' \circ \widehat{\psi}$ are not isomorphic (since $\mathrm{End}(E')$ has no non-trivial units).

The isogeny ϕ factors as $\psi_2 \circ \psi \circ \psi_1$ and so $\widehat{\phi}$ factors as $\widehat{\psi_1} \circ \widehat{\psi} \circ \widehat{\psi_2}$. Since the isogeny up is always unique, we have that ψ_1 and $\widehat{\psi_2}$ are uniquely determined. However, the isogenies ψ_2 and $\widehat{\psi_1}$ are only constrained by the condition that the full composition has cyclic kernel.

We now give a few results which show how the above ideas can be used to give information about Heegner points on $X_0^+(N)$.

Proposition 12. *Let N be an integer greater than one and $\mathcal{O}$ an order of discriminant D and conductor c divisible by 2. Suppose that $(\frac{D/c^2}{2}) = +1$. Then a Heegner point of $X_0(N)$ of discriminant D can arise only if N/c^2 is even.*

Proof. Suppose instead that N/c^2 is odd and that we have a Heegner point on $X_0(N)$. Without loss of generality we may assume $c = 2$.

The isogeny ϕ factors as $\psi_2 \circ \psi \circ \psi_1$ where ψ_1 is an isogeny up of degree 2 and ψ_2 is an isogeny down. Indeed, since N/c^2 is odd we may instead factor ϕ as $\psi' \circ \psi_2 \circ \psi_1$.

Since $(\frac{D/c^2}{2}) = +1$ the choice of the isogeny ψ_2 down is unique. It follows that $\psi_2 \cong \widehat{\psi_1}$ and therefore the isogeny does not have cyclic kernel. □

In Section 10 the case $N = 64$ and $D = -28$ appears. This is an interesting example of how a rational point of $X_0^+(N)$ can arise when both c and N/c^2 are even.

It is useful to know when a Heegner point is fixed by an Atkin-Lehner involution. We give one result in this direction which can apply when p is 2 or 3.

Proposition 13. *Suppose $\phi : E \to E'$ is a Heegner point on $X_0^+(N)$ of discriminant D and having prime conductor p. Suppose that the class number of D is one, that $p^2 \| N$ and that $p - (\frac{D/p^2}{p}) = 2$. Then the Heegner point is fixed by the Atkin-Lehner involution W_{p^2}.*

Proof. Write $N = p^2 m$. Since the class number of D is one it follows that $E \cong E'$. We can factor ϕ as $\psi_2 \circ \psi_1 \circ \psi$ where ψ_1 is a p-isogeny up and ψ_2 is a p-isogeny down and ψ has degree m. Since $p - (\frac{D/p^2}{p}) = 2$ there are only two choices for the isogeny down. It follows that ψ_2 is uniquely specified by the condition $\psi_2 \neq \widehat{\psi_1}$.

It remains to show that the m-isogeny ψ is fixed by W_{p^2} (this argument is applies in more general cases too). Let τ correspond to the Heegner point, so that $NA\tau^2 + B\tau + C = 0$ where $B^2 - 4NAC = D$. We focus on the isogeny ψ given as $(\mathbb{C}/\langle 1, \tau\rangle, \langle 1/m, \tau\rangle)$. The class number one condition implies that $W_{p^2}(\tau) = \gamma(\tau)$ for some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Using the quadratic equation for τ one can deduce that $\gamma \in \Gamma_0(m)$ and that the isogeny ψ is preserved.

Therefore, the involution W_{p^2} must fix the Heegner point. □

An example of the above situation occurs with $N = 52$ and $D = -16$. We have $p = 2$, $(\frac{-4}{2}) = 0$ and there is only one rational Heegner point on $X_0^+(52)$ corresponding to the discriminant -16. In contrast, with $N = 52$ and $D = -12$ we have $(\frac{-3}{2}) = -1$ and there are two rational Heegner points on $X_0^+(52)$ arising (each mapped to the other by W_4).

In the cases where there is more than one Heegner point of a given discriminant arising it is interesting to know whether they are mapped to each other by certain Atkin-Lehner involutions.

Proposition 14. *Let D be a discriminant of an order $\mathcal{O}$ of class number one and suppose that the conductor of $\mathcal{O}$ is a prime p. Let N be an integer such that $p^2|N$ and suppose there are rational Heegner points on $X_0^+(N)$ of discriminant D. Let α be such that $p^\alpha \| N$. Then these Heegner points are mapped to each other by the Atkin-Lehner involution W_{p^α}.*

Proof. The candidates for D are $-12, -16, -27$ and -28 and so p is equal to either 2 or 3. All rational Heegner points must correspond to isogenies $\psi_2 \circ \psi \circ \psi_1$. The isogeny ψ_1 is unique and there are at most two choices each for ψ and ψ_2. Hence there can be at most two rational Heegner points arising.

Let τ be such that $(\mathbb{C}/\langle 1, \tau\rangle, \langle 1/N, \tau\rangle)$ corresponds to one of these two Heegner points. So τ satisfies some polynomial $NA\tau^2 + B\tau + C = 0$ where $B^2 - 4NAC = D$. From $p^2|N$ and $p^2|D$ it follows that $p|B$. Write p^α for the exact power of p dividing N. By considering the cases one can show that $p^\alpha \not| B$.

Consider the action of W_{p^α} on τ. From the class number one hypothesis we have $W_{p^\alpha}(\tau) = \gamma(\tau)$ for some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Write $W_{p^\alpha} = \left(\begin{smallmatrix} p^\alpha a & b \\ Nc & p^\alpha d \end{smallmatrix}\right)$ and $\gamma = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$. Then $W_{p^\alpha}(\tau) = \gamma(\tau)$ implies

$$(p^\alpha at - Ncr)\tau^2 + (p^\alpha au + bt - p^\alpha rd + Nsc)\tau + (bu - p^\alpha sd) = 0.$$

Comparing this with $NA\tau^2 + B\tau + C = 0$ we have that $N/p^\alpha | t$ and $p|t$. Since $p^\alpha \not| B$ it follows that $p^\alpha \not| t$. Therefore $\gamma \notin \Gamma_0(N)$.

Write $p^\beta \| t$ (so $1 \leq \beta < \alpha$). We have that W_{p^α} has mapped the Heegner point to $(\mathbb{C}/\langle 1, \tau\rangle, \langle (1 + Np^{\beta-\alpha}\tau)/N, \tau\rangle)$ which is evidently not $\Gamma_0(N)$-isomorphic to $\langle 1/N, \tau\rangle$ or $\langle 1, \tau/N\rangle$. Thus we have shown that W_{p^α} maps the one Heegner point on $X_0^+(N)$ to the other one. □

One sees that it is possible to state results about the action of the Atkin-Lehner involutions on Heegner points, but that the amount of work involved is inordinate compared with the case when N is coprime to the conductor of the order. As a result, we refrain from stating any further such results.

We mention that in any specific example it is easy to determine whether τ and $W_n(\tau)$ are $\Gamma_0(N)$-equivalent for any $n|N$.

It seems likely that all rational Heegner points on $X_0^+(N)$, corresponding to discriminants D of class number two are fixed by all the Atkin-Lehner involutions.

Proposition 15. *Let $N > 89$, then there are no rational Heegner points on $X_0^+(N)$ corresponding to elliptic curves whose endomorphism ring has class number two.*

Proof. Suppose we have a Heegner point on $X_0^+(N)$ of discriminant D. The case where $\gcd(N, c) = 1$ has been handled in Proposition 8, so we assume that $\gcd(N, c) \neq 1$ and that we have some isogenies up and down of degree d (where d

divides c). It follows that $N|D$. It remains to determine which possible values for N can arise with $d > 1$.

The only 'large' values for D with non-trivial conductor are $D = -72, -75, -99, -100, -112$ and -147 (for which we have $c = 3, 5, 3, 5, 4$ and 7 respectively).

The possibilities for $N > 89$ are therefore $99, 100, 112$ and 147. These cases do not have rational points since the corresponding ideal $\mathfrak{n}$ would necessarily be principal. □

As we have seen, $X_0^+(89)$ has a class number two Heegner point. Rational Heegner points corresponding to class number two discriminants for which N is not coprime to the conductor seem to be extremely rare. In fact, the only example I know occurs with $N = 8$ and $D = -32$.

9. Results of Momose

Momose [25], [26] has studied the question of whether there are exceptional rational points on $X_0^+(N)$.

Theorem 6. *(Momose [26]) Let N be a composite number. If any one of the following conditions holds then $X_0^+(N)(\mathbb{Q})$ has no exceptional rational points (i.e., all rational points of $X_0^+(N)$ are cusps, rational points of $X_0(N)$, or Heegner points).*

1. *N has a prime divisor p such that $p \geq 11, p \neq 13, 37$ and $\#J_0^-(p)(\mathbb{Q})$ finite.*
2. *The genus of $X_0^+(N)$ is at least 1 and N is divisible by $26, 27$ or 35.*
3. *The genus of $X_0^+(N)$ is at least 1, N is divisible by 49, and $m := N/49$ is such that one of the following three conditions holds: 7 or 9 divides m; a prime $q \equiv -1 \pmod 3$ divides m; or m is not divisible by 7 and $(\frac{-7}{m}) = -1$.*

Regarding the first condition above, Momose states that the number of points of $\#J_0^-(p)(\mathbb{Q})$ is finite for $p = 11$ and all primes $17 \leq p \leq 300$ except 151, 199, 227 and 277.

Of course, when the genus of $X_0^+(N)$ is zero then there will be infinitely many exceptional rational points. The N for which this occurs are $N \leq 21$, $23 \leq N \leq 27$, $29, 31, 32, 35, 36, 39, 41, 47, 49, 50, 59$ and 71 (see Ogg [29]). Information about the quadratic $\mathbb{Q}$-curves in the cases $N = 2, 3, 5, 7$ and 13 was found by Hasegawa [20]. González and Lario [13] determined the j-invariants of $\mathbb{Q}$-curves when $X_0^*(N)$ has genus zero or one and so their results also contain all these cases of quadratic $\mathbb{Q}$-curves (although their results give polyquadratic j-invariants and the quadratic cases are not readily distinguishable from the others).

It is also possible to have infinitely many exceptional points in the case when the genus of $X_0^+(N)$ is one.

10. Genus one cases

It can be shown (see González and Lario [13] Section 3 for the square-free case) that $X_0^+(N)$ has genus one when N is $22, 28, 30, 33, 34, 37,\ 38, 40, 43, 44, 45, 48, 51,\ 53, 54, 55, 56, 61, 63, 64, 65, 75, 79, 81, 83, 89, 95, 101, 119$ and 131. In the cases $37, 43, 53, 61, 65, 79, 83, 89, 101$ and 131 the rank of the elliptic curve $X_0^+(N)$ is one and so there are infinitely many rational points.

A particularly interesting case in the context of this paper is that of 65, since it is the only value above which is not prime. Thus there are infinitely many quadratic j-invariants of elliptic curves which are 65-isogenous to their Galois conjugate.

It would be interesting to know how many of these 65-isogenous $\mathbb{Q}$-curves also admit an n-isogeny for some smaller n. In fact, what happens in general with all quadratic $\mathbb{Q}$-curves when the isogeny has large degree?

For the remaining cases the rank of the elliptic curve is zero and we can ask whether the only points are cusps and Heegner points. Momose's result covers many of these cases and so the only N we must consider are $28, 30, 40, 45, 48$, $56, 63, 64$ and 75. The following table lists the results and we see that there are no exceptional rational points in these cases. Note that in this case, unlike the other tables in this paper, the number of rational points on $X_0^+(N)$ is known to be correct.

N	$X_0^+(N)$ (see [5])	# $\mathbb{Q}$-points	# $\mathbb{Q}$-cusps	Heegner point D
28	14 A4(A)	6	3	One $D = -7$, two $D = -12$
30	15 A8(A)	4	4	None
40	20 A2(A)	6	4	Two $D = -16$
45	15 A8(A)	4	2	Two $D = -11$
48	24 A4(A)	4	4	None
56	14 A4(A)	6	4	One each $D = -7, -28$
63	21 A4(A)	4	2	Two $D = -27$
64	32 A2(A)	4	2	One each $D = -7, -28$.
75	15 A8(A)	4	2	Two $D = -11$

11. Higher genus cases

We now turn attention to the values of N for which the genus of $X_0^+(N)$ is two or more. For these cases there are only finitely many rational points. The following table lists all the values of N for which the genus of $X_0^+(N)$ is between 2 and 5 and for which Momose's theorem does not apply.

Genus	N
2	42, 72, 74, 80, 91, 111, 125
3	60, 96, 100, 128, 169
4	84, 90, 117
5	112, 144, 185

We now embark on a computational study of these cases using the methods of [9], [10].

The results are given in the following table. Note that the number in the second column is not proven to be correct; it is simply the number of points of low height found by a simple search as in [10]. Nevertheless, we conjecture that this is the correct number of points in each case.

N	$\#X_0^+(N)(\mathbb{Q})$	# cusps	Heegner points
42	4	4	None.
60	6	6	None.
72	4	4	None.
74	6	2	Two $D=-7$, one each $D=-4,-148$.
80	4	4	None.
84	8	6	Two $D=-12$.
90	4	4	None.
91	10	2	Has exceptional points, see Section 12.
96	4	4	None.
100	4	3	One $D=-16$.
111	6	2	Two $D=-11$, one each $D=-3,-12$.
112	6	4	One each $D=-7,-28$.
117	4	2	Two $D=-27$.
125	6	1	Has exceptional points, see Section 13.
128	4	2	One each $D=-7,-28$.
144	4	4	None.
169	7	1	One each $D=-3,-4,-12,-16,-27,-43$.
185	8	2	Two each $D=-4,-11,-16$.

12. The case $N = 91 = 7 \cdot 13$

In this case there are exceptional rational points. We give the details of the calculations in this case and we exhibit the j-invariants of the corresponding quadratic $\mathbb{Q}$-curves.

A basis for the weight two forms on $\Gamma_0(91)$ which have eigenvalue $+1$ with respect to W_{91} is given (see [4]) by the two forms

$$\begin{aligned} f &= q - 2q^3 - 2q^4 - 3q^5 + q^7 + q^9 + 4q^{12} + q^{13} + \cdots \\ g &= q - 2q^2 + 2q^4 - 3q^5 - q^7 - 3q^9 + 6q^{10} - 6q^{11} - q^{13} + \cdots \end{aligned}$$

Following the techniques of [12], [27], [19], [9] we set $h = (f-g)/2$, $x = f/h$ and $y = -q(dx/dq)/h$ and find the equation

$$y^2 = x^6 - 4x^5 + 4x^4 - 4x^3 + 12x^2 - 12x + 4$$

for $X_0^+(91)$. The hyperelliptic involution is not an Atkin-Lehner involution in this case and so we find ourselves in an analogous situation to the case $X_0(37)$.

There are two rational cusps on $X_0^+(91)$ and three candidate discriminants $D = -3, -12$ and -27 for Heegner points. The primes 7 and 13 both split in each of the orders of these discriminants and so there are always two rational Heegner points for each of them.

The Heegner point of discriminant -91 does not give a rational point since the corresponding ramified ideal is principal.

It is easy to find 10 points on the model above, which confirms that there are two exceptional rational points on $X_0^+(91)$.

The Atkin-Lehner involution W_7 (which is equivalent to W_{13} on $X_0^+(91)$) maps the exceptional points to each other. It can be shown by considering the original modular forms that W_7 maps a point (x, y) to $(x/(x-1), y/(x-1)^3)$.

The following table lists all the data.

Point	Discriminant
$+\infty$	Cusp ∞
$-\infty$	$D = -12$
$(0, 2)$	$D = -27$
$(0, -2)$	$D = -27$
$(1, 1)$	Cusp $[1/7]$
$(1, -1)$	$D = -12$
$(3, 7)$	Exceptional
$(3, -7)$	$D = -3$
$(3/2, 7/8)$	Exceptional
$(3/2, -7/8)$	$D = -3$

The exceptional points correspond to quadratic $\mathbb{Q}$-curves as in Section 5. The j-invariants can be computed using the method of Elkies [8]. The point $(3, 7)$ corresponds to the elliptic curve having j-invariant equal to

$$-27048390693611915236875/2^{14} \pm 6098504215856136863625/2^{14}\sqrt{-3 \cdot 29}.$$

The point $(3/2, 7/8)$ corresponds to the elliptic curve having j-invariant equal to

$$836687744296472061804988681612 5/2^{92} \pm 32028251460268098916979319375/2^{92}\sqrt{-3 \cdot 29}.$$

We comment that the powers 14 and 92 in the denominators follow the pattern $14 = 13+1$ and $92 = 91+1$ which suggests an analogue of Theorem 3.2 of González [14].

As in [10] and [14] we observe that these j-invariants have some properties similar to those enjoyed by the singular j-invariants (see Gross and Zagier [18]).

Also note that the j-invariants are of the form $\alpha/2^{13}$ and $\alpha'/2^{91}$ where α, α are algebraic integers such that the norms satisfy $\gcd(N(\alpha), 2^{13}) = 2^{7-1}$ and $\gcd(N(\alpha'), 2^{91}) = 2^{91-1}$.

We list some of these properties below (here $N(j)$ represents the norm over the quadratic extension, while 'Coefficient' means the coefficient of $\sqrt{-3 \cdot 29}$ in the j-invariant).

$N(j_1)$	$2^{-20} \cdot 3^2 \cdot 5^6 \cdot 7^5 \cdot 17^3 \cdot 199^3 \cdot 55326353^3$
$N(j_2)$	$2^{-92} \cdot 3^2 \cdot 5^6 \cdot 7^5 \cdot 17^3 \cdot 199^3 \cdot 53681^3$
$N(j_1 - 1728)$	$2^{-20} \cdot 3^2 \cdot 373^2 \cdot 3297787^2 \cdot 1066779696251^2$
$N(j_2 - 1728)$	$2^{-92} \cdot 3^2 \cdot 23^4 \cdot 373^2 \cdot 8496368633^2$
Coefficient	$2^{-14} \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11 \cdot 19 \cdot 23 \cdot 53 \cdot 67 \cdot 71 \cdot 101 \cdot 103 \cdot 239 \cdot 257$
Coefficient	$2^{-92} \cdot 3^3 \cdot 5^4 \cdot 7 \cdot 11 \cdot 19 \cdot 23 \cdot 43 \cdot 61 \cdot 71 \cdot 131 \cdot 241 \cdot 313 \cdot 701 \cdot 1901$

We see, as usual, that $N(j)$ is 'nearly a cube' and that $N(j - 1728)$ is square. Notice the similarities in the primes arising above. Also note that the 'coefficient' is divisible by 7 in both cases but not 13.

13. The case $N = 125$

We are again in the situation where $X_0^+(N)$ is genus two and where the hyperelliptic involution is not an Atkin-Lehner involution. An equation for $X_0^+(125)$ is

$$y^2 = x^6 + 2x^5 + 5x^4 + 10x^3 + 10x^2 + 8x + 1.$$

We find six rational points on the curve. There is one rational cusp, and we get Heegner points for each of the discriminants $D = -4, -11, -16$ and -19. In each

case there is only one Heegner point. It follows that there is an exceptional point. We first give the table of points.

Point	Explanation
∞	Cusp
$-\infty$	$D = -19$
$(0, 1)$	$D = -11$
$(0, -1)$	$D = -16$
$(-2, 5)$	Exceptional
$(-2, -5)$	$D = -4$

As usual the exceptional rational point corresponds to a quadratic $\mathbb{Q}$-curve. We calculate the j-invariant of the curve to be

$$-2140988208276499951039156514868631437312/11^5$$
$$\pm 948976338978410928412003346760125644 80/11^5\sqrt{509}.$$

The following factorisations occur.

$N(j)$	$2^{36} \cdot 3^6 \cdot 11^{-6} \cdot 175465901521^3$
$N(j - 1728)$	$2^{12} \cdot 3^{12} \cdot 5^8 \cdot 7^4 \cdot 11^{-6} \cdot 2741^2$
Coefficient	$2^{20} \cdot 3^7 \cdot 5 \cdot 7^3 \cdot 11^{-5} \cdot 13 \cdot 17 \cdot 19 \cdot 29 \cdot 31 \cdot 59 \cdot 101 \cdot 113$
of $\sqrt{509}$	$\cdot 131 \cdot 179 \cdot 463 \cdot 563 \cdot 1553$

The j-invariant is of the form $\alpha/11^5$ where α is an algebraic integer and the norm of α satisfies $\gcd(N(\alpha), 11^5) = 11^{5-1}$.

References

1. A. O. L. Atkin, J. Lehner, *Hecke Operators on* $\Gamma_0(N)$, Math. Ann., **185**, p. 134–160 (1970)
2. B. J. Birch, W. Kuyk (eds.), *Modular Functions of One Variable IV*, Springer-Verlag LNM 476 (1975)
3. B. J. Birch, *Heegner points of elliptic curves*, AMS Symp. math. 15, Inf. teor., Strutt. Corpi algebr., Convegni 1973, p. 441–445 (1975)
4. H. Cohen, N.-P. Skoruppa and D. Zagier, *Tables of modular forms*, Preprint (1992)
5. J. E. Cremona, *Algorithms for modular elliptic curves*, Cambridge (1992)
6. P. Deligne, M. Rappoport, *Les schemas de modules de courbes elliptiques*, in Modular Functions one Variable II, Springer Lecture Notes Math. 349, p. 143–316 (1973)
7. N. Elkies, *Remarks on elliptic K-curves*, preprint (1993)
8. N. Elkies, *Elliptic and modular curves over finite fields and related computational issues*, in D. A. Buell and J. T. Teitelbaum (eds.), Computational Perspectives on Number Theory, AMS Studies in Advanced Math., p. 21–76 (1998)
9. S. D. Galbraith, *Equations for Modular Curves*, Doctoral Thesis, Oxford (1996)
10. S. D. Galbraith, *Rational points on* $X_0^+(p)$, Experimental Mathematics, **8**, No. 4, p. 311–318 (1999)
11. S. D. Galbraith, *Constructing isogenies between elliptic curves over finite fields*, London Math. Soc. J. Comp. Math., **2**, p. 118–138 (1999)
12. J. González, *Equations of hyperelliptic modular curves*, Ann. Inst. Fourier, 41, , p. 779-795 (1991)
13. J. González, J.-C. Lario, *Rational and elliptic parametrizations of* $\mathbb{Q}$*-curves*, J. Number Theory **72**, No.1, p. 13–31 (1998)
14. J. González, *On the j-invariants of the quadratic* $\mathbb{Q}$*-curves*, Preprint (1999)
15. B. H. Gross, *Arithmetic on elliptic curves with complex multiplication*, Springer LNM Mathematics 776 (1980)
16. B. H. Gross, *Heegner Points on* $X_0(N)$, in Modular Forms, R. A. Rankin (ed.), Wiley, p. 87–105 (1984)
17. B. H. Gross, *Heegner points and the modular curve of prime level*, J. Math. Soc. Japan, **39**, No. 2, p. 345–362 (1987)

18. B. H. Gross, D. B. Zagier, *On singular moduli*, J. Reine Angew. Math., **355**, p. 191–220 (1985)
19. Y. Hasegawa, *Table of quotient curves of modular curves $X_0(N)$ with genus 2*, Proc. Japan Acad., Ser. A, **71**, No.10, p. 235–239 (1995)
20. Y. Hasegawa, $\mathbb{Q}$*-curves over quadratic fields*, Manuscripta Math. **94**, no. 3, p. 347–364 (1997)
21. M. A. Kenku, *On the Modular Curves $X_0(125), X_0(25)$ and $X_0(49)$*, J. London Math. Soc., **23**, p. 415–427 (1981)
22. S. Lang, *Algebraic number theory*, 2nd edition, Springer GTM 110, (1970)
23. S. Lang, *Elliptic Functions*, 2nd edition, Springer GTM 112 (1987)
24. B. Mazur, *Modular Curves and the Eisenstein Ideal*, Pub. I.H.E.S, **47**, p. 33–186 (1977)
25. F. Momose, *Rational Points on $X_0^+(p^r)$*, J. Faculty of Science University of Tokyo Section 1A Mathematics, **33** no.3, p. 441–466 (1986)
26. F. Momose, *Rational Points on the Modular Curves $X_0^+(N)$*, J. Math. Soc. Japan, **39**, no.2, p. 269–285 (1987)
27. N. Murabayashi. *On normal forms of modular curves of genus 2*, Osaka J. Math. **29**, No.2, p. 405–418 (1992)
28. A. Ogg, *Rational Points on Certain Elliptic Modular Curves*, in H. Diamond (ed.), AMS Proc. Symp, Pure Math., v. **24**, p. 221–231 (1973)
29. A. Ogg, *Hyperelliptic Modular Curves*, Bull. Soc. Math. France, **102**, p. 449–462 (1974)
30. K. Ribet, *Abelian varieties over $\mathbb{Q}$ and modular forms*, Proceedings of KAIST workshop, p. 53–79 (1992)
31. J.H. Silverman, *Introduction to the Theory of Elliptic Curves*, Springer GTM 106, (1986)
32. M. Shimura, *Defining equations of modular curves $X_0(N)$*, Tokyo J. Math., **18**, No.2, p. 443–456 (1995)

IEM, Ellernstr. 29, 45326 Essen, Germany.
E-mail address: galbra@exp-math.uni-essen.de