Journal de Théorie des Nombres
de Bordeaux **14** (2002), 205–219

Rational points on $X_0^+(N)$ and quadratic $\mathbb{Q}$-curves

par Steven D. GALBRAITH

Résumé. Nous considérons les points rationnels sur $X_0(N)/W_N$ dans le cas où N est un nombre composé. Nous faisons une étude de certains cas qui ne se déduisent pas des résultats de Momose. Des points rationnels sont obtenus pour $N = 91$ et $N = 125$. Nous exhibons aussi les j-invariants des $\mathbb{Q}$-courbes quadratiques correspondantes.

Abstract. The rational points on $X_0(N)/W_N$ in the case where N is a composite number are considered. A computational study of some of the cases not covered by the results of Momose is given. Exceptional rational points are found in the cases $N = 91$ and $N = 125$ and the j-invariants of the corresponding quadratic $\mathbb{Q}$-curves are exhibited.

1. Introduction

Let N be an integer greater than one and consider the modular curve $X_0(N)$ whose non-cusp points correspond to isomorphism classes of isogenies between elliptic curves $\phi : E \to E'$ of degree N with cyclic kernel [5]. The rational points of $X_0(N)$ have been studied by many authors. Results of Mazur [21], Kenku [19] and others have provided a classification of them. The conclusion is that rational points usually arise from cusps or elliptic curves with complex multiplication. There are a finite number of values of N for which other rational points arise, and we call such rational points 'exceptional'. For $X_0(N)$ the largest N for which there are exceptional rational points is the famous case $N = 37$.

The Fricke involution W_N on $X_0(N)$ arises from taking the dual isogeny $\widehat{\phi} : E' \to E$. 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. There is a model for $X_0^+(N)$ over $\mathbb{Q}$ and one can study the $\mathbb{Q}$-rational points on this curve.

Rational points on $X_0^+(N)$ are an interesting object of study. Momose [22], [23] has given some results of a similar nature to those of Mazur,

Manuscrit reçu le 2 septembre 2000.

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 [9] which gave a computational study of the case when N is a prime number.

The conclusions of this work and [9] are the following: The modular curve $X_0^+(N)$ has an exceptional rational point when $N \in \{73, 91, 103, 125, 137, 191, 311\}$. We conjecture that these are the only values of N for which the genus of $X_0^+(N)$ is between 2 and 5 and for which $X_0^+(N)$ has exceptional rational points. The above conjecture includes the statement that $X_{\mathrm{split}}(p)$ (which is isomorphic to $X_0^+(p^2)$) has no exceptional rational points when $p = 13$.

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

The case of cusps can be easily understood. Rational cusps on $X_0(N)$ give rise to rational cusps on $X_0^+(N)$. Using the notation for cusps introduced by Ogg [25], the following result easily follows.

Proposition 1. *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 $\{[1 : \sqrt{N}], [-1 : \sqrt{N}]\}$.*

The non-cusp points of $X_0^+(N)$ can be interpreted as pairs $\{\phi : E \to E', \widehat{\phi} : E' \to E\}$. From [5] 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: Either the rational point is a cusp, or else it 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, $E \ncong E'$, and the non-trivial element $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ is such that $\phi^\sigma \cong \widehat{\phi}$ and $E' \cong E^\sigma$.

Case 1 is the case of rational points on $X_0(N)$, and these have been classified. Rational points on $X_0(N)$ corresponding to elliptic curves with complex multiplication can arise as Heegner points (see Section 3) or not (e.g., the case of $X_0(14)$ where there is an isogeny $\phi : E \to E'$ of degree 14 such that $\mathrm{End}(E)$ has discriminant -28 while $\mathrm{End}(E')$ has discriminant -7).

In case 2 above we have $E \cong E'$ and so $\mathrm{End}(E) \cong \mathrm{End}(E')$. The existence of a cyclic isogeny of degree N implies that the elliptic curves have complex multiplication and so the point is a Heegner point (and the class number of the endomorphism ring is one).

In case 3 there are two possibilities: either E has complex multiplication (and therefore $\mathrm{End}(E) \cong \mathrm{End}(E')$ and the point is a Heegner point of class number two) or not, in which case we call the point an exceptional rational point. In both cases we have an elliptic curve E over a quadratic field (and not defined over $\mathbb{Q}$) which is isogenous to its Galois conjugate. Such an elliptic curve is called a 'quadratic $\mathbb{Q}$-curve' (see [14], [27]).

Examples of quadratic $\mathbb{Q}$-curves which do not have complex multiplication are interesting and one of the main contributions of this paper is to provide some new examples of these.

It can be shown that every quadratic $\mathbb{Q}$-curve without complex multiplication corresponds to a rational point on $X_0^+(N)$ for some $N > 1$. For a more general result along these lines see Elkies [6].

We now recall the definition of the Atkin-Lehner involutions [1] for any $n|N$ such that $\gcd(n, N/n) = 1$. Over $\mathbb{C}$ they may be defined as elements of $\mathrm{SL}_2(\mathbb{R})$ 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 acts non-trivially 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.

Proposition 2. *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 size $2^{\omega(N)-1}$. The field of definition of the corresponding j-invariants is the same for all the exceptional points in a given orbit.*

Proof. Suppose we have a point of $X_0^+(N)$ which is fixed by some Atkin-Lehner involution W_n. Such a point corresponds to some $\tau \in \mathcal{H}^*$ such that $W_n(\tau) = \gamma(\tau)$ (or $W_{N/n}(\tau) = \gamma(\tau)$) 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 and the point is not exceptional.

The field of definition of the j-invariants is the field of definition of the points on $X_0(N)$ which correspond to the rational point on $X_0^+(N)$. Since the action of W_n is rational on $X_0(N)$ it follows that the field of definition is preserved. $\square$

3. Heegner points

A Heegner point of $X_0(N)$ [2] 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.

It is well-known (see [2], [15], [9]) that 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 $\gcd(NA, B, C) = \gcd(A, B, NC) = 1$. The correspondence 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 [20] 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 conductor of an order of discriminant D is the index of the order in the maximal order of $\mathbb{Q}(\sqrt{D})$ and it may be computed as the largest positive integer c such that $D/c^2 \equiv 0, 1 \pmod 4$.

We must recall a few well-known facts about isogenies of degree dividing the conductor c (see the Appendix of [10] for an elementary proof). 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 there are exactly p isogenies of degree p from E 'down' to elliptic curves whose endomorphism ring has discriminant $p^2 D$. 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 $p^2 D$.

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

Proposition 3. *Suppose $\phi : E \to E'$ 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 $p^2|N$ (this also follows from the fact that 'what goes up must come down'). 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 $p\tau$ is a root of the quadratic $(NA/p^2)X^2+(B/p)X+C$, 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).

The following result is now clear.

Proposition 4. *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 are Heegner points on $X_0(N)$ corresponding to the order $\mathcal{O}$ only if* $\gcd(N/d^2,c/d)=1$, *all primes $p|(N/d^2)$ are such that $(\frac{D/d^2}{p})\neq -1$ and all primes p such that $p^2|(N/d^2)$ are such that $(\frac{D/d^2}{p})=+1$.*

Proof. If $p|\gcd(N/d^2,c/d)$ then there must be some p-isogeny up which is not matched by a p-isogeny back down again and it follows that the corresponding point of $X_0(N)$ is not a Heegner point.

The conditions on primes p dividing N/d^2 come from the fact that kernel of the corresponding p-isogeny can be viewed as an ideal. For the composition of these isogenies to have cyclic kernel it follows that the primes must split or ramify and that ramified primes can only occur with multiplicity one. □

The next result gives further constraints on when a Heegner point can exist.

Proposition 5. *Let N be an integer greater than one and $\mathcal{O}$ an order of discriminant D and conductor c. Suppose that $2^a\|c$, that $(\frac{D/2^{2a}}{2})=+1$, and that $2^{2a}|N$. Then a Heegner point of $X_0(N)$ of discriminant D can arise only if $2^{2a+1}|N$.*

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

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. $\square$

In Section 7 the case $N = 64$ and $D = -28$ appears. This is an example of how a rational point of $X_0^+(N)$ can arise when both c and N/c^2 are even.

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 $X_0^+(N)$.

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

In the context of this paper it is important to determine when Heegner points on $X_0(N)$ can give a rational point of $X_0^+(N)$.

Following Gross [15] 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 $\langle N, (-B + \sqrt{D})/2\rangle$. 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.

From the results of Gross one can easily deduce the following (see [9]).

Theorem 1. *Let $x = \{\phi : E \to E', \widehat{\phi} : E' \to E\}$ 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 $\mathfrak{n} = \overline{\mathfrak{n}}$.*

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.

As seen in [9], rational Heegner points coming from class number two orders are rather rare.

Proposition 6. *Suppose $N > 89$. Then there are no rational Heegner points on $X_0^+(N)$ of class number two.*

Proof. Let D be the discriminant of a class number two discriminant. We consider first the case when N is coprime to the conductor of D.

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 $D = -267$.

Now, assume that $\gcd(N, c) \neq 1$ and that we have some isogenies up and down of degree d (where d divides c). The remaining N/d^2 isogeny is handled by the previous case, and so it follows that $N|D$. It remains to determine which possible values for N can arise with $d > 1$.

The only values for D with non-trivial conductor are $D = -32, -36, -48, -60\ -64, -72, -75,\ -99,\ -100, -112$ and -147 (for which we have $c = 2, 3, 4, 2, 4, 3, 5, 3,\ 5, 4$ 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 mentioned above, $X_0^+(89)$ 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 have noticed occurs with $N = 8$ and $D = -32$. There are further examples of rational Heegner points of class number two. For instance, in Section 8 it is shown that the curve $X_0^+(74)$ is an example of a composite value of N for which there is a rational class number two heegner point.

We could end the analysis here, since Proposition 4 and the fact that Heegner points come from quadratic forms $NA\tau^2 + B\tau + C$ of discriminant D can be used as the basis of an algorithm to list all $\Gamma_0(N)$-equivalence classes of suitable τ and Theorem 1 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, it is useful to have more information about the action of the Atkin-Lehner involutions on Heegner points.

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

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

Proposition 7 (Gross [15]). *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 8. *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. Furthermore $\omega'(N) = 0$ and the point is fixed by all the Atkin-Lehner involutions.*

Proof. From 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 7 and Theorem 1. □

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

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.

It follows that there may be several non-isomorphic Heegner points coming from a given discriminant D. 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 (which are the most commonly encountered cases).

Proposition 9. *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} (the argument we give 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. $\square$

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).

6. Results of Momose

Momose [22], [23] has studied the question of whether there are exceptional rational points on $X_0^+(N)$.

Theorem 2 (Momose [23]). *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 [26]). Information about the quadratic $\mathbb{Q}$-curves in the cases $N = 2, 3, 5, 7$ and 13 was found by Hasegawa [18]. González and Lario [12] 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.

7. Genus one cases

It can be shown (see González and Lario [12] 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 exceptional rational points.

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 table the number of rational points on $X_0^+(N)$ is known to be correct.

N	$X_0^+(N)$ (*)	# $\mathbb{Q}$-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 $D = -11$

(*) see [4].

8. 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 composite 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. The prime cases have already been studied in [9].

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 [8], [9]. The key is to construct explicit equations for $X_0^+(N)$ using the techniques of [11], [24] and [28] and cusp form data from [3].

The results are given in the following table. The value for $\#X_0^+(N)(\mathbb{Q})$ given in the second column is proven to be correct in many cases by using coverings to rank zero elliptic curves. Nevertheless, for the cases $N \in \{91, 117, 125, 169, 185\}$ it is simply the number of points of low height found by a search as in [9]. 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 9.
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 10.
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 $D = -4, -11, -16$.

9. 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 [3]) 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 [11], [24], [17], [8] 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	Explanation
$+\infty$	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. The j-invariants can be computed using the method of Elkies [7]. The point $(3, 7)$ corresponds to the elliptic curve having j-invariant equal to

$$j_1 = -27048390693611915236875/2^{14} \pm 6098504215856136863625/2^{14}\sqrt{-3\cdot 29}.$$

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

$$j_2 = 83668774429647206180498868 16125/2^{92} \pm 320282514602680989169793193 75/2^{92}\sqrt{-3\cdot 29}.$$

As in [9] and [13] it is seen that these j-invariants have some properties similar to those enjoyed by the singular j-invariants (see Gross and Zagier [16]). 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 j_1	$2^{-14}\cdot 3^2\cdot 5^3\cdot 7\cdot 11\cdot 19\cdot 23\cdot 53\cdot 67\cdot 71\cdot 101\cdot 103\cdot 239\cdot 257$
Coefficient j_2	$2^{-92}\cdot 3^3\cdot 5^4\cdot 7\cdot 11\cdot 19\cdot 23^2\cdot 43\cdot 61\cdot 71\cdot 131\cdot 241\cdot 313\cdot 701\cdot 1901$

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, and that the 'coefficient' is divisible by 7 in both cases but not 13.

Also note that the j-invariants are of the form $j_1=\alpha/2^{13}$ and $j_2=\alpha'/2^{91}$ where α,α' are algebraic integers such that the norms satisfy $\gcd(N(\alpha), 2^{13})=2^{7-1}$ and $\gcd(N(\alpha'),2^{91})=2^{91-1}$. This suggests an analogue of Theorem 3.2 of González [13].

10. The case $N=125$

We are again in the situation where $X_0^+(N)$ has genus two and where the hyperelliptic involution is not an Atkin-Lehner involution. From [3] we find that the following forms are a basis for the weight two cusp forms for $\Gamma_0^+(N)$

$$\begin{aligned} f &= q-q^2-q^3-3q^7+q^8-q^9-3q^{11}+q^{12}-3q^{13}+\cdots \\ g &= q^2-q^3-q^4-q^6-2q^8+3q^9+2q^{12}+3q^{13}+\cdots . \end{aligned}$$

Taking functions $x=f/g$ and $y=-q(dx/dq)/g$ gives the following equation for $X_0^+(125)$

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

We find six rational points on the curve. There is one rational cusp, and we find 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
$-\infty$	$D=-19$
$(0,1)$	$D=-16$
$(0,-1)$	$D=-11$
$(-2,5)$	$D=-4$
$(-2,-5)$	Exceptional

The exceptional rational point corresponds to a quadratic $\mathbb{Q}$-curve with

$$j = -21409882082764999510391565148686314373 12/11^5$$
$$\pm 948976338978410928412003346760125644 80/11^5\sqrt{509}.$$

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 of $\sqrt{509}$	$2^{20}\cdot 3^7\cdot 5\cdot 7^3\cdot 11^{-5}\cdot 13\cdot 17\cdot 19\cdot 29\cdot 31\cdot 59\cdot 101\cdot 113$ $\cdot 131\cdot 179\cdot 463\cdot 563\cdot 1553$

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

Acknowledgements

This research was supported by the EPSRC, the Centre for Applied Cryptographic Research at the University of Waterloo, the NRW-Initiative für Wissenschaft und Wirtschaft "Innovationscluster für Neue Medien", and cv cryptovision gmbh (Gelsenkirchen).

I thank the referee for their careful reading of the paper.

References

[1] A. O. L. ATKIN, J. LEHNER, *Hecke Operators on* $\Gamma_0(N)$, Math. Ann. **185** (1970), 134–160.

[2] B. J. BIRCH, *Heegner points of elliptic curves*, AMS Symp. math. **15** (1975), Inf. teor., Strutt. Corpi algebr., Convegni 1973, 441–445.

[3] H. COHEN, N.-P. SKORUPPA, D. ZAGIER, *Tables of modular forms.* Preprint, 1992.

[4] J. E. CREMONA, *Algorithms for modular elliptic curves.* Cambridge (1992)

[5] P. DELIGNE, M. RAPPOPORT, *Les schemas de modules de courbes elliptiques.* In Modular Functions one Variable II, Springer Lecture Notes Math. **349** (1973), 143–316.

[6] N. ELKIES, *Remarks on elliptic K-curves*, preprint, 1993.

[7] 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., 1998, 21–76.

[8] S. D. GALBRAITH, *Equations for Modular Curves.* Doctoral Thesis, Oxford, 1996.

[9] S. D. GALBRAITH, *Rational points on $X_0^+(p)$.* Experiment. Math. **8** (1999), 311–318.

[10] S. D. GALBRAITH, *Constructing isogenies between elliptic curves over finite fields.* London Math. Soc. J. Comp. Math. **2** (1999), 118–138.

[11] J. GONZÁLEZ, *Equations of hyperelliptic modular curves.* Ann. Inst. Fourier bf41 (1991), 779–795.

[12] J. GONZÁLEZ, J.-C. LARIO, *Rational and elliptic parametrizations of $\mathbb{Q}$-curves.* J. Number Theory **72** (1998), 13–31.

[13] J. GONZÁLEZ, *On the j-invariants of the quadratic $\mathbb{Q}$-curves.* J. London Math. Soc. **63** (2001), 52–68.

[14] B. H. GROSS, *Arithmetic on elliptic curves with complex multiplication.* Lect. Notes Mathematics **776**, Springer, 1980.

[15] B. H. GROSS, *Heegner Points on $X_0(N)$.* In Modular Forms, R. A. Rankin (ed.), Wiley, 1984, 87–105.

[16] B. H. GROSS, D. B. ZAGIER, *On singular moduli.* J. Reine Angew. Math. **355** (1985), 191–220.

[17] Y. Hasegawa, *Table of quotient curves of modular curves $X_0(N)$ with genus 2.* Proc. Japan Acad. Ser. A **71** (1995), 235–239.

[18] Y. Hasegawa, *$\mathbb{Q}$-curves over quadratic fields.* Manuscripta Math. **94** (1997), 347–364.

[19] M. A. Kenku, *On the Modular Curves $X_0(125), X_0(25)$ and $X_0(49)$.* J. London Math. Soc. **23** (1981), 415–427.

[20] S. Lang, *Elliptic Functions*, 2nd edition. Springer GTM 112, 1987.

[21] B. Mazur, *Modular Curves and the Eisenstein Ideal.* Pub. I.H.E.S, **47** (1977), 33–186.

[22] F. Momose, *Rational Points on $X_0^+(p^r)$.* J. Faculty of Science University of Tokyo Section 1A Mathematics **33** (1986), 441–466.

[23] F. Momose, *Rational Points on the Modular Curves $X_0^+(N)$.* J. Math. Soc. Japan **39** (1987), 269–285.

[24] N. Murabayashi, *On normal forms of modular curves of genus 2.* Osaka J. Math. **29** (1992), 405–418.

[25] A. Ogg, *Rational Points on Certain Elliptic Modular Curves.* In H. Diamond (ed.), AMS Proc. Symp. Pure Math. **24**, 1973, 221–231.

[26] A. Ogg, *Hyperelliptic Modular Curves.* Bull. Soc. Math. France **102** (1974), 449–462.

[27] K. Ribet, *Abelian varieties over $\mathbb{Q}$ and modular forms.* Proceedings of KAIST workshop (1992), 53–79.

[28] M. Shimura, *Defining equations of modular curves $X_0(N)$.* Tokyo J. Math. **18** (1995), 443–456.

Steven D. Galbraith
Mathematics Department
Royal Holloway University of London
Egham, Surrey TW20 OEX, UK
E-mail : `Steven.Galbraith@rhul.ac.uk`